COMPREHENSIVE INTERNET SECURITY™

SonicWALL Security Appliance

SonicOS Standard 3.0 Administrator's Guide

SONICWALL

Table of Contents

Table of Contents i

Preface xi
    Copyright Notice xi
    Trademarks xi
    Limited Warranty xii
  About this Guide xiii
    Organization of this Guide xiv
    Guide Conventions xvi
    Icons Used in this Manual xvi
  SonicWALL Technical Support xvii
  More Information on SonicWALL Products and Services xvii

PART 1: Introduction

Chapter 1: Introduction 3
  What's New in SonicOS Standard 3.0 3
  SonicWALL Management Interface 4
    Navigating the Management Interface 5
    Status Bar 6
    Applying Changes 6
    Navigating Tables 6
    Common Icons in the Management Interface 7
    Getting Help 7
    Logging Out 7

Chapter 2: Basic SonicWALL Security Appliance Setup 9
  Collecting Required ISP Information 9
    Internet Service Provider (ISP) Information 9
    Other Information 10
  Accessing the SonicWALL Security Appliance Management Interface 11
  Using the SonicWALL Setup Wizard 11
    SonicWALL TZ 170 SP 11
    SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless 12
    Configuring a Static IP Address Internet Connection 12
    Configuring a DHCP Internet Connection 14
    Configuring a PPPoE Internet Connection 14
    Configuring PPTP Internet Connectivity 15
    Configuring the TZ 170 SP using the Setup Wizard 17
    Configuring the TZ 50 Wireless/TZ 150 Wireless/170 Wireless using the Setup Wizard . 18
    Configuring the TZ 50 Wireless/TZ 150 Wireless/170 Wireless as an Office Gateway . . 18
    Configuring the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless
      as a Secure Access Point 20
    Configuring the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless
      as a Guest Internet Gateway 21
    Configuring the TZ 170 Wireless as a Secure Wireless Bridge 22

Registering Your SonicWALL Security Appliance 24
  Before You Register 24
  Creating a mySonicWALL.com Account 24
  Registering Your SonicWALL Security Appliance 25

PART 2: System

Chapter 3: Viewing System Status Information 29
System > Status 29
  Wizards 30
  System Messages 30
  System Information 30
  Security Services 31
  Latest Alerts 31
  Network Interfaces 32

Chapter 4: System > Licenses 33
System > Licenses 33
  Node License Status 34
  Node License Exclusion List 34
  Security Services Summary 35
  Manage Security Services Online 36
  Manual Upgrade 36
  Manual Upgrade for Closed Environments 36

Chapter 5: Using System Administration 39
System > Administration 39
  Firewall Name 40
  Name/Password 40
  Login Security 40
  Web Management Settings 41
  Advanced Management 42

Chapter 6: Setting System Time 45
System > Time 45
  Set Time 45
  NTP Settings 46

Chapter 7: Configuring System Settings 47
System > Settings 47
  Settings 47
  Firmware Management 48
  SafeMode - Rebooting the SonicWALL Security Appliance 49

Chapter 8: Performing Diagnostic Tests and Restarting the SonicWALL Security Appliance51
System > Diagnostics 51
  Tech Support Report 52
  Diagnostic Tools 53
  Active Connections Monitor 53
  CPU Monitor 54
  DNS Name Lookup 54
  Find Network Path 55
  Packet Trace 55

Ping 57
Process Monitor 57
Reverse Name Resolution 57
System > Restart 58

PART 3: Network

Chapter 9: Configuring Network Settings 61
Network > Settings 61
Setup Wizard 62
Interfaces 62
DNS Settings 63
Configuring the WAN Interface 64
Configuring Transparent Mode. 64
Configuring NAT Enabled. 66
Configuring NAT with DHCP Client 66
Configuring NAT with PPPoE Client. 67
Configuring NAT with L2TP Client 67
Configuring NAT with PPTP Client. 68
Configuring Ethernet Settings in WAN Properties 68
Configuring the LAN Interface 70
Basic LAN Configuration 70
Configuring Multiple LAN Subnets 70
Configuring Ethernet Settings 71
Configuring the OPT Interface. 71
Configuring Transparent Mode. 72
Configuring NAT Mode. 73
Configuring the DMZ Interface 73
Configuring Transparent Mode. 74
Configuring NAT Mode. 75
Configuring the Modem Interface (TZ 170 SP) 75
Failover. 77
Advanced 78
Activating the Modem. 78
Configuring WLAN Properties (TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless) 79

Chapter 10: Configuring One-to-One NAT 81
Network > One-to-One NAT 81
One-to-One NAT Configuration Example. 82

Chapter 11: Configuring Web Proxy Settings 85
Network > Web Proxy 85
Configuring Automatic Web Proxy Forwarding 86
Bypass Proxy Servers Upon Proxy Failure 86
Forward OPT/DMZ/WLAN Client Requests to Proxy Server 86

Chapter 12: Configuring Intranet Settings 87
Network > Intranet 87
Installation 88
Intranet Settings 88

Chapter 13:Configuring Static Routes 89
  Network > Routing 89
    Static Routes 90
    Route Advertisement 91
    Routing Table 92

Chapter 14:Configuring Address Resolution Protocol Settings. 93
  Network > ARP 93
    Static ARP Entries 94
    Secondary Subnets with Static ARP 94
    Prohibit Dynamic ARP Entries 96
    Navigating and Sorting the ARP Cache Table 97
    Flushing the ARP Cache 97

Chapter 15:Configuring the DHCP Server 99
  Network > DHCP Server 99
    DHCP Server Settings 99
    DHCP Server Lease Scopes 100
    Configuring DHCP Server for Dynamic Ranges 100
    Configuring Static DHCP Entries 101
    Current DHCP Leases 102

Chapter 16:Configuring Dynamic DNS 103
  Network > Dynamic DNS 103
    Supported DDNS Providers 103
    Configuring Dynamic DNS 105
    Dynamic DNS Settings Table 107

PART 4: Modem

Chapter 17:Viewing Modem Status 111
  Modem > Status 111
    Modem Status 112

Chapter 18:Configuring Modem Settings 113
  Modem > Settings 113
    Configuring Profile and Modem Settings 114

Chapter 19:Configuring Modem Failover 115
  Modem > Failover 115
    Modem Failover Settings 115
    Configuring Modem Failover 116

Chapter 20:Configuring Advanced Modem Settings 117
  Modem > Advanced 117

Chapter 21:Configuring Modem Dialup Properties 119
  Modem > Dialup Profiles 119
    Dial-Up Profiles 119
    Configuring a Dialup Profile 120
  Modem > Dialup Profiles > Modem Profile Configuration 120
    Configuring a Dialup Profile 120
    Chat Scripts 123

PART 5: Wireless

Chapter 22: Setting Up the WLAN Using the Wireless Wizard and Monitoring Your WLAN 127

Considerations for Using Wireless Connections 128
Optimal Wireless Performance Recommendations. 129
  Adjusting the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless Antennas. 129
  Wireless Guest Services (WGS) 129
  Wireless Node Count Enforcement 130
  MAC Filter List 130
  WiFiSec Enforcement. 130
Using the Wireless Wizard 131
Wireless > Status. 135
  WLAN Settings. 136
  WLAN Statistics 137
  Station Status. 137

Chapter 23: Configuring Wireless Settings 139
Wireless > Settings 139
  Wireless Radio Mode 139
  Wireless Settings 140
  Secure Wireless Bridging (TZ 170 Only) 141
  Configuring a Secure Wireless Bridge 142

Chapter 24: Configuring WEP and WPA Encryption 147
Wireless > WEP/WPA Encryption 147
  WEP Encryption Settings 148
  WEP Encryption Keys 148
  WPA Encryption Settings 148

Chapter 25: Configuring Advanced Wireless Settings. 151
Wireless > Advanced. 151
  Beaconing & SSID Controls 151
  Wireless Client Communications 152
  Advanced Radio Settings. 152

Chapter 26: Configuring the MAC Filter List 155
Wireless > MAC Filter List 155

Chapter 27: Configuring Wireless IDS. 157
Wireless > IDS. 157

PART 6: Wireless Guest Services

Chapter 28: Viewing Wireless Guest Services Status. 163
WGS > Status 163

Chapter 29: Configuring Wireless Guest Services 165
WGS > Settings. 165
  Bypass Guest Authentication 166
  Bypass Filters for Guest Accounts 166
  Enable Dynamic Address Translation (DAT) 166
  Enable SMTP Redirect. 167
  Enable URL Allow List for Authenticated Users 167
  Enable IP Address Deny List for Authenticated Users. 167

Customize Login Page 168
Custom Post Authentication Redirect Page 169
Maximum Concurrent Guests 169
WGS Account Profiles 169

Chapter 30:Managing Wireless Guest Accounts 171
WGS > Accounts 171
Working with Guest Accounts 171
Automatically Generating Guest Accounts 172
Manually Configuring Wireless Guests 173
Flexible Default Route 174
Secure Access Point with Wireless Guest Services 175

PART 7: Firewall

Chapter 31:Configuring Network Access Rules 179
Network Access Rules Overview 179
Using Bandwidth Management with Access Rules. 180
Firewall > Access Rules 180
Restoring Default Network Access Rules 181
Adding Rules using the Network Access Rule Wizard 181
Configuring a Public Server Rule 181
Configuring a General Network Access Rule 182
Adding Rules Using the Add Rule Window 184
Rule Examples 187

Chapter 32:Configuring Advanced Rule Options 189
Access Rules > Advanced 189
Windows Networking (NetBIOS) Broadcast Pass Through. 189
Detection Prevention 190
Source Routed Packets. 190
TCP Connection Inactivity Timeout 190
TCP Checksum Validation. 190
Access Rule Service Options 190

Chapter 33:Configuring Custom Services. 191
Firewall > Services 191
User Defined (Custom) Services. 191
Predefined Services 192

Chapter 34:Configuring VoIP 193
Firewall > VoIP 193
VoIP Protocols. 193
Configuring the VoIP Settings 195

Chapter 35:Monitoring Active Firewall Connections 197
Firewall > Connections Monitor 197
Setting Filter Logic. 198
Using Group Filters 198

PART 8: VPN

Chapter 36:Configuring VPN Settings. 201
SonicWALL VPN Options Overview 201

- VPN > Settings . . . 202
  - VPN Global Settings . . . 202
  - VPN Policies . . . 202
  - Currently Active VPN Tunnels . . . 203
- Configuring GroupVPN Policy on the SonicWALL . . . 203
  - Configuring IKE Preshared Secret . . . 204
  - Configuring GroupVPN with IKE 3rd Party Certificates . . . 208
  - Export a GroupVPN Client Policy . . . 213
- Site to Site VPN Configurations . . . 213
  - Site-to-Site VPN Deployments . . . 213
  - VPN Planning Sheet for Site-to-Site VPN Policies . . . 214
  - Configuring Site to Site VPN Policies Using the VPN Policy Wizard . . . 215
  - Creating a Typical IKE Preshared Secret VPN Policy . . . 216
  - Creating a Custom VPN Policy IKE with Preshared Secret . . . 217
  - Creating a Manual Key VPN Policy with the VPN Policy Wizard . . . 218
  - Configuring IKE 3rd Party Certificates with the VPN Policy Wizard . . . 219
  - Creating Site-to-Site VPN Policies Using the VPN Policy Window . . . 220

Chapter 37:Configuring Advanced VPN Settings . . . 229

- VPN > Advanced . . . 229
  - Advanced VPN Settings . . . 229
  - VPN User Authentication Settings . . . 230
  - VPN Bandwidth Management . . . 231

Chapter 38:Configuring DHCP Over VPN . . . 233

- VPN > DHCP over VPN . . . 233
  - DHCP Relay Mode . . . 233
  - Configuring the Central Gateway for DHCP Over VPN . . . 234
  - Configuring DHCP over VPN Remote Gateway . . . 235
  - Device Configuration . . . 236
  - Current DHCP over VPN Leases . . . 236

Chapter 39:Configuring L2TP Server Settings . . . 237

- VPN > L2TP Server . . . 237
  - L2TP Server Settings . . . 238
  - IP Address Settings . . . 238
  - Adding L2TP Clients to the SonicWALL . . . 238
  - Currently Active L2TP Sessions . . . 239

Chapter 40:Managing Certificates . . . 241

- Digital Certificates Overview . . . 241
  - SonicWALL Third-Party Digital Certificate Support . . . 241
- VPN > Local Certificates . . . 242
  - Importing Certificate with Private Key . . . 242
  - Certificate Details . . . 242
  - Generating a Certificate Signing Request . . . 243
- VPN > CA Certificates . . . 244
  - Importing CA Certificates into the SonicWALL . . . 244
  - Certificate Details . . . 244
  - Certificate Revocation List (CRL) . . . 245

PART 9: Users

Chapter 41:Viewing User Status and Configuring User Authentication. . . . 249
- User Level Authentication Overview 249
- Users > Status 249
  - Active User Sessions 250
- Users > Settings 250
  - Authentication Method 250
  - Global User Settings 251
  - Internet Authentication Exclusions 251
  - Acceptable Use Policy 252
  - Configuring RADIUS Authentication 253

Chapter 42:Configuring Local Users 257
- Users > Local Users 257
  - Adding a Local User 258

PART 10: Security Services

Chapter 43:Managing SonicWALL Security Services 261
- SonicWALL Security Services 261
  - mySonicWALL.com 262
  - Activating Free Trials 262
- Security Services > Summary 263
  - Security Services Summary 263
  - Manage Licenses 263
  - If Your SonicWALL Security Appliance is Not Registered 264
  - Security Services Settings 264
  - Security Services Information 264

Chapter 44:Configuring SonicWALL Content Filtering Service 265
- SonicWALL Content Filtering Service 265
- Security Services > Content Filter 266
  - Content Filter Status 266
  - Activating SonicWALL Content Filtering Service 266
  - Activating a SonicWALL Content Filtering Service FREE TRIAL 267
  - Content Filter Type 268
  - Restrict Web Features 268
  - Trusted Domains 269
  - Message to Display when Blocking 269
- Configuring SonicWALL Filter Properties 269
  - Custom List 270
  - Settings 271
  - Consent 272
  - Mandatory Filtered IP Addresses 273

Chapter 45:Managing SonicWALL Network Anti-Virus and E-Mail Filter Services275
- SonicWALL Network Anti-Virus Overview 275
- Security Services > Anti-Virus 276
  - Activating SonicWALL Network Anti-Virus 276
  - Activating a SonicWALL Network Anti-Virus FREE TRIAL 277
- Security Services > E-Mail Filter 278

Configuring SonicWALL Network
Anti-Virus 278

Chapter 46: Managing SonicWALL Gateway Anti-Virus Service. 279
SonicWALL Gateway Anti-Virus Overview 279
Configuring SonicWALL Gateway
Anti-Virus 283

Chapter 47: Managing SonicWALL Intrusion Prevention Service 285
SonicWALL Intrusion Prevention Service 285
SonicWALL IPS Features. 285
SonicWALL Deep Packet Inspection 286
How SonicWALL's Deep Packet Inspection Architecture Works 287
Security Services > Intrusion Prevention. 288
Activating SonicWALL IPS 288
Activating the SonicWALL IPS FREE TRIAL 289

Chapter 48: Managing SonicWALL Global Security Client 291
SonicWALL Global Security Client 291
Global Security Client Features 292
How SonicWALL Global Security Client Works 292
SonicWALL Global Security Client Activation 292
Activating SonicWALL Global Security Client 293

PART 11: Log

Chapter 49: Viewing Log Events 297
SonicOS Log Event Messages Overview 297
Log > View. 298
Navigating and Sorting Log View Table Entries. 298
SonicOS Log Entries 299

Chapter 50: Specifying Log Categories. 301
Log > Categories 301
Log Categories. 301
Alerts & SNMP Traps 302

Chapter 51: Configuring Log Automation 303
Log > Automation 303
E-mail 304
Syslog Servers 304

Chapter 52: Configuring Name Resolution 307
Log > Name Resolution. 307
Selecting Name Resolution Settings 308
Specifying the DNS Server. 308

Chapter 53: Generating and Viewing Log Reports 309
Log > Reports 309
Data Collection. 309
View Data. 310
Log > ViewPoint 311
SonicWALL ViewPoint 311

Appendix A:Using the SonicSetup Diagnostic and Recovery Tool 313
SonicSetup 313
Introduction and Discovery 314
Device Selection 314
Diagnostics 315
Diagnostic Results. 316
SonicROM Recovery 316
SonicOS Recovery 317
Restoring Factory Defaults 318
Address Synchronization 319

Appendix B:Resetting the SonicWALL Security Appliance Using SafeMode321
SonicWALL SafeMode 321
Upgrading SonicOS Firmware 323

Index 325

Preface

Copyright Notice

© 2004 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

About this Guide

Welcome to the *SonicWALL SonicOS Standard 3.0 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Standard 3.0 on the following SonicWALL security appliance:

SonicWALL TZ 50
SonicWALL TZ 50 Wireless
SonicWALL TZ 150
SonicWALL TZ 150 Wireless
SonicWALL TZ 170
SonicWALL TZ 170 SP
SonicWALL TZ 170 Wireless
SonicWALL PRO 1260
SonicWALL PRO 2040
SonicWALL PRO 3060

Note: *For the latest version of this manual as well as other SonicWALL product documentation, refer to <http//:www.sonicwall.com/services/documentation.html>.*

Tip: *The* ***Getting Start Guide*** *for your SonicWALL security appliance provides instructions for installing and configuring your SonicWALL security appliance for connecting your network through the SonicWALL security appliance for secure Internet connectivity.*

Organization of this Guide

The SonicOS Standard 3.0 Administrator's Guide organization is structured into the following parts that parallel the top-level menu items of SonicWALL Web-based management interface. Within these parts, individual chapters correspond to the specific configuration pages listed as submenu items in the management interface.

Part 1 Introduction

This part provides an overview of the SonicWALL management interface conventions, explains how to get your network securely connected to the Internet with the SonicWALL security appliance using the Setup Wizard, and registering your SonicWALL security appliance.

Part 2 System

This part covers the configuration of a variety SonicWALL security appliance controls for managing system status information, registering the SonicWALL security appliance, activating and managing SonicWALL Security Services licenses, configuring SonicWALL security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 3 Network

This part provides instructions for configuring the SonicWALL security appliance for your network environment. It explains configuring network interface settings manually, setting up a DHCP server, configuring the Web proxy requests to a network proxy server, configuring static routes and ARP settings, and configuring dynamic DNS.

Part 4 Modem (TZ 170 SP)

This part explains how to configure the SonicWALL TZ 170 SP's built-in modem for use as the primary Internet connection or as a dial-up failover for the primary broadband Internet connection.

Part 5 Wireless (TZ 150 Wireless/TZ 170 Wireless)

This part explains how to set up the SonicWALL TZ 150 Wireless/TZ 170 Wireless for secure WiFiSec or WEP/WPA Internet access, configure wireless intrusion detection settings, and configure wireless clients for secure wireless and remote access via the SonicWALl Global VPN Client.

Part 6 Wireless Guest Services (TZ 150 Wireless/TZ 170 Wireless)

This part explains how configure wireless guest accounts for the SonicWALL TZ 150 Wireless/TZ 170 Wireless to securely support wireless network guests.

Part 7 Firewall

This part explains how to configure and manage firewall access policies to deny or permit traffic, how to configure Voice over IP (VoIP) traffic to pass through, and monitor active firewall connections.

Part 8 VPN

This part covers how to create VPN policies on the SonicWALL security appliance to support SonicWALL Global VPN Clients for remote client access, as well as site-to-site VPN policies for connecting Loans between offices running SonicWALL security appliances.

Part 9 Users

This part explains how to create and manage a user database on the SonicWALL security appliance.

and how to integrate the SonicWALL security appliance with a RADIUS server for user authentication.

Part 10 Security Services

This part includes an overview of optional SonicWALL security services. When combined with network security features of the SonicWALL security appliance, these services provide comprehensive protection against a wide range of threats, including viruses, worms, Trojans, spyware, peer-to-peer and instant messaging application exploits, malicious code, and inappropriate or unproductive web sites.

These subscription-based services include SonicWALL Content Filtering Service, SonicWALL Network Anti-Virus, Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, and SonicWALL Global Security Client. FREE trials of many of these these security service subscriptions are available after you register your SonicWALL security appliance.

Part 11 Log

This part covers managing the SonicWALL security appliance's enhanced logging, alerting, and reporting features. The SonicWALL security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

Guide Conventions

The following Conventions used in this guide are as follows:

Convention	**Use**
Bold	Highlights items you can select on the SonicWALL management interface.
Italic	Highlights a value to enter into a field. For example, "type *192.168.168.168* in the **IP Address** field."
Menu Item > Menu Item	Indicates a multiple step management interface menu choice. For example, **Security Services > Content Filter** means select **Security Services**, then select **Content Filter**.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

▲ **Alert:** *Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL security appliance.*

✓ **Tip:** *Useful information about security features and configurations on your SonicWALL security appliance.*

✎ **Note:** *Important information on a feature that requires callout for special attention.*

➲ **Cross Reference:** *Pointer to related or more detailed information on the topic.*

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at *<http://www.sonicwall.com/services/support.html>*. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Australia - + 1800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39.02.7541.9803

Japan - + 81(0)3.5460.5356

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41.1.308.3.977

UK - +44(0)1344.668.484

Note: *Please visit <http://www.sonicwall.com/services/contact.html> for the latest technical support telephone numbers.*

More Information on SonicWALL Products and Services

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408) 745-9300

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

http://www.sonicwall.com/services/documentation.html

PART

1

Introduction

CHAPTER

1

Introduction

What’s New in SonicOS Standard 3.0

- **Real-time Gateway Anti Virus (GAV)** - Provides per packet virus scanning using a Deep Packet Inspection version 2.0 engine. The Real-time GAV feature provides over 4,500 signatures on the SonicWALL TZ series security appliances and over 24,000 signatures on the SonicWALL PRO series governing gateway appliances. The Real-time GAV feature supports zip and gzip data compression. The Real-time GAV feature supports scanning the following message delivery protocols:
  - HyperText Transport Protocol (HTTP)
  - Simple Mail Transfer Protocol (SMTP)
  - Internet Message Access Protocol (IMAP)
  - Post Office Protocol 3 (POP3)
  - File Transfer Protocol (FTP)
  - Transmission Control Protocol (TCP) packet streams
- **IPS 2.0** - Includes an updated Data Packet Inspection (DPI) engine that powers Intrusion Prevention Services (IPS) and GAV. The IPS version 2.0 engine includes the following feature enhancements:
  - **IP Fragmentation** - Provides the ability to either disallow IP fragments or to reassemble IP fragments for full application layer inspection.
  - **Checksum Validation** - Provides the ability to detect and prevent invalid IP, ICMP, TCP, and UDP checksums.
  - **Global IP Exclusion List** - Provides the ability to configure a range of IP addresses to exclude specified network traffic from IPS evaluation.
  - **Log Redundancy** - Provides the ability to configure per-category and per-signature log redundancy filter settings.
  - **Dynamic Categorization** - Groups and displays signatures automatically in expandable category views. Category maintenance is performed through automated signature updates.
- **Enhanced VoIP Support** - Adds comprehensive support for third-party VoIP equipment, including products from Cisco, Mitel, Pingtel, Grandstream, Polycom, D-Link, Pulver, Apple iChat, and softphones from Yahoo, Microsoft, Ubiquity, and OpenPhone. Enhanced VoIP support adds the ability to handle SIP, H.323v1, H.323v2, H.323v3, and H.323v4. The internal DHCP Server capability in SonicOS Standard 2.6 allows any SIP endpoint to receive addressing information into the DHCP scope information, this enables any SIP endpoint to receive SIP Proxy addresses when they issue a DHCP request on the network.

Note: *Registration Admission Status (RAS) and Internet Locator Service (ILS) LDAP for H.323 is not supported on SonicOS Standard 3.0. For H.323 RAS and ILS LDAP support on the SonicWALL TZ 170 Series, upgrade your firmware to SonicOS Enhanced 3.0 (or greater). For H.323 RAS and ILS LDAP support on the SonicWALL PRO 2040 or SonicWALL PRO 3060, upgrade your firmware to SonicOS Enhanced 2.5 (or greater).*

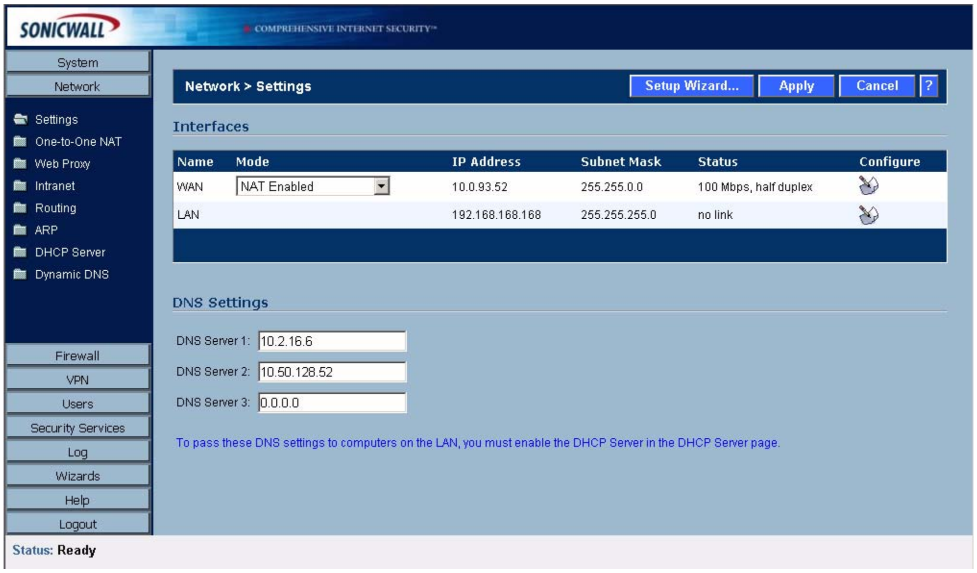
- **Dynamic DNS** - Enables the SonicWALL security device to dynamically register its WAN IP address with a Dynamic Domain Name Server (DDNS) service provider.
- **Lightweight Hotspot Messaging** - Provides Hotspot users authentication between a SonicWALL wireless access device (such as a SonicWALL TZ 170 Wireless, or a SonicPoint with a SonicWALL PRO series governing gateway appliance) and an Authentication Back-End (ABE) for parametrically bound network access.
- **Wireless Radio Operating Schedul**e - Provides the ability to create a schedule to control the operation of the wireless radio for SonicWALL wireless access devices (such as the SonicWALL TZ 170 Wireless or SonicPoint).
- **WiFiSec Exception List** - Provides wireless users the flexibility to bypass WiFiSec enforcement. The WiFiSec Exception List enables you to allow NT Domain logons to occur prior to Global VPN Client (GVC) tunnel establishment.
- **Real-time Monitoring** - Includes the following monitoring tools:
  - **CPU Monitor** allows you to generate CPU utilization reports in a customizable histogram format.
  - **Process Monitor** allows you to generate reports on current running processes.
  - **Active Connections Monitor** allows you to generate reports on current active network connections.
- **DHCP Server Enhancements** - Includes expanded hash tables for resource management, accelerated duplicate-address detection, and improved Dynamic Host Configuration Protocol (DHCP) Server internal-database maintenance management.
- **Expanded Logging** - Includes additional logging capabilities to provide expanded flexibility. You can export the log into plain text or CSV values. Logging categories are dramatically expanded, the logs conform to Syslog severity levels so you can set the SonicWALL security appliance to only log alerts and messages of specified levels. And you can independently specify which categories are logged to the internal log. When directing logs to external Syslog servers, you can rate-limit the messages based on events-per-second or maximum bytes-per-second, so that external Syslog servers do not become overwhelmed.
- **Static ARP Support** - Enables you to create static Address Resolution Protocol (ARP) entries, create MAC address to IP address bindings, and to publish static ARP entries for use in a secondary network subnet.
- **Virtual Adapter Static IP Support** - Provides support for static IP addressing of Global VPN Client (GVC) virtual adapters.

SonicWALL Management Interface

The SonicWALL security appliance’s Web-based management interface provides a easy-to-use graphical interface for configuring your SonicWALL security appliance. The following provides an overview of the key management interface objects.

Navigating the Management Interface

Navigating the SonicWALL management interface includes a hierarchy of menu buttons on the navigation bar (left side of your browser window).


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Dynamic DNS
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Network > Settings
Setup Wizard...
Apply
Cancel
?
Status: Ready

Interfaces

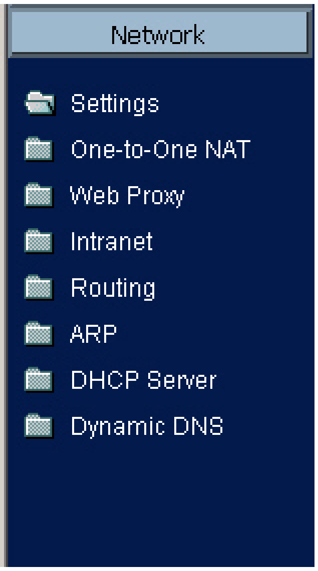
Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.52	255.255.0.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	no link	

DNS Settings

DNS Server 1: 10.2.16.6
DNS Server 2: 10.50.128.52
DNS Server 3: 0.0.0.0

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the DHCP Server page.

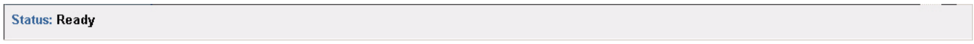
When you click a menu button, related management functions are displayed as submenu items in the navigation bar.


Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Dynamic DNS

To navigate to a submenu page, click the link. When you click a menu button, the first submenu item page is displayed. The first submenu page is automatically displayed when you click the menu button. For example, when you click the **Network** button, the **Network > Settings** page is displayed.

Status Bar

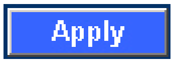
The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicWALL management interface.



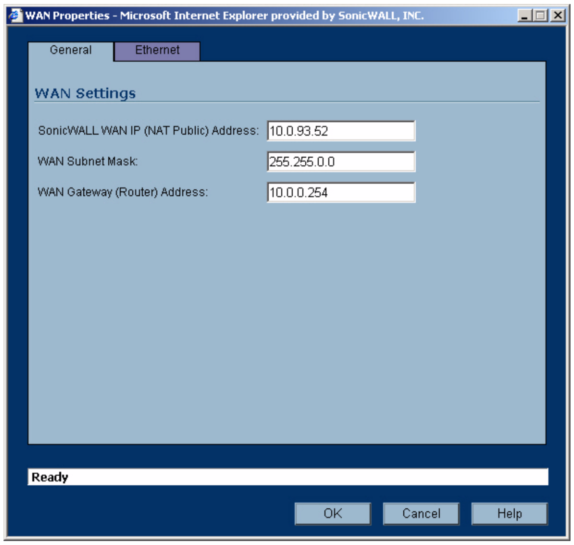
Status: Ready

Applying Changes

Click the **Apply** button at the top right corner of the SonicWALL management interface to save any configuration changes you made on the page.



If the settings are contained in a secondary window within the management interface, when you click **OK**, the settings are automatically applied to the SonicWALL security appliance.

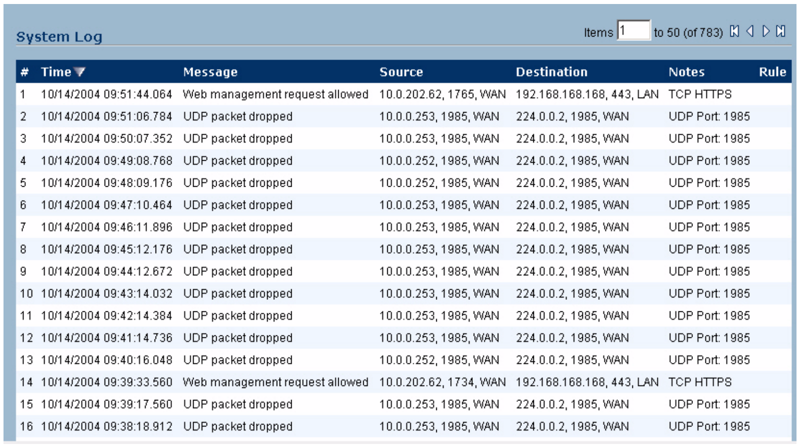

WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
WAN Settings
OK
Cancel
Help

SonicWALL WAN IP (NAT Public) Address: 10.0.93.52
WAN Subnet Mask: 255.255.0.0
WAN Gateway (Router) Address: 10.0.0.254

Ready

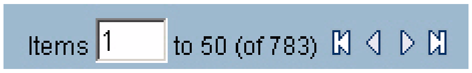
Navigating Tables

Navigate tables in the management interface with large number of entries by using the navigation buttons located on the upper right top corner of the table.



#	Time	Message	Source	Destination	Notes	Rule
1	10/14/2004 09:51:44.064	Web management request allowed	10.0.202.62, 1765, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
2	10/14/2004 09:51:06.784	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
3	10/14/2004 09:50:07.352	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
4	10/14/2004 09:49:08.768	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
5	10/14/2004 09:48:09.176	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
6	10/14/2004 09:47:10.464	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
7	10/14/2004 09:46:11.896	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
8	10/14/2004 09:45:12.176	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
9	10/14/2004 09:44:12.672	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
10	10/14/2004 09:43:14.032	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
11	10/14/2004 09:42:14.384	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
12	10/14/2004 09:41:14.736	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
13	10/14/2004 09:40:16.048	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
14	10/14/2004 09:39:33.560	Web management request allowed	10.0.202.62, 1734, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
15	10/14/2004 09:39:17.560	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
16	10/14/2004 09:38:18.912	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	

The table navigation bar includes buttons for moving through table pages.



Common Icons in the Management Interface

The following describe the functions of common icons used in the SonicWALL management interface:

Clicking on the edit ✎ icon displays a window for editing the settings.

Clicking on the delete 🗑 icon deletes a table entry

Moving the pointer over the comment 💬 icon displays text from a Comment field entry.

Getting Help

Each SonicWALL security appliance includes Web-based on-line help available from the management interface.

Clicking the question mark **?** button on the top-right corner of every page accesses the context-sensitive help for the page.

▲ **Alert:** *Accessing the SonicWALL security appliance online help requires an active Internet connection.*

Logging Out

The **Logout** button at the bottom of the menu bar terminates the management interface session and displays the authentication page for logging into the SonicWALL security appliance.

CHAPTER

2

Basic SonicWALL Security Appliance Setup

SonicWALL Security Appliance Configuration Steps

The chapter provides instructions for basic installation of the SonicWALL security appliance running SonicOS Standard 3.0. After you complete this chapter, computers on your LAN will have secure Internet Internet access.

- “Collecting Required ISP Information” on page 9
- “Accessing the SonicWALL Security Appliance Management Interface” on page 11
- “Using the SonicWALL Setup Wizard” on page 11
- “Registering Your SonicWALL Security Appliance” on page 24

Collecting Required ISP Information

Before you configure your SonicWALL security appliance for Internet connectivity for your computers, make sure you have any information required for your type of Internet connection available.

Internet Service Provider (ISP) Information

If You Have a Cable Modem

Your ISP is probably using DHCP to dynamically assign an address to your computer.

You do not need any Internet connection information.

If You Have DSL

Your ISP is probably using PPPoE to dynamically authenticate your login and assign an address to your computer. You will need:

User Name: ____________________________

Note: *Your ISP may require your user name to include the "@" symbol and the domain name, for example, "Joe@sonicwall.com"*

Password:____________________________

If You Have a Static IP Address

Your ISP may have assigned you a static IP address for your computer. If so, the paperwork or e-mail confirmation from your ISP should contain the following configuration information:

IP Address: ____________________________

Subnet Mask: ____________________________

Default Gateway: ____________________________

Primary DNS: ____________________________

Secondary DNS (optional): ____________________________

If Your ISP Provided You With a Server IP Address, User Name, and Password

Your ISP may be using PPTP to establish a secure connection between your computer and a server. You will need:

Server Address: ____________________________

User Name: ____________________________

Password: ____________________________

If you are unsure what kind of connection you have, the paperwork or e-mail confirmation message from your ISP should contain the information. If you cannot find the information, you can rely on the SonicWALL security appliance to automatically detect the correct settings during setup.

Other Information

SonicWALL Management Interface

To access the SonicWALL security appliance Web-based management interface. These are the default settings, which you can change:

User Name: *admin*

Password: *password*

Note: *If you are not using one of the network configurations above, refer to Chapter 3, Configuring Network Settings.*

Accessing the SonicWALL Security Appliance Management Interface

To access the Web-based management interface of the SonicWALL security appliance:

1. On the computer you have connected to a network port, start your Web browser.

Alert: *Your Web browser must support Java and HTTP uploads. Internet Explorer 5.0 or higher or Netscape Navigator 4.7 or higher are recommended.*

2. Enter **192.168.168.168** in the **Location** or **Address** field. The first time you access the SonicWALL management interface, the SonicWALL **Setup Wizard** launches and guides you through the configuration and setup of your SonicWALL security appliance.
3. If the **Setup Wizard** does not display, the **System > Status** page is displayed. Click the **Setup Wizard** button on the **Network > Settings** page.
4. Proceed to one of the following configuration options for your type of Internet connection:

- “Configuring a Static IP Address Internet Connection” on page 12
- “Configuring a DHCP Internet Connection” on page 14
- “Configuring a PPPoE Internet Connection” on page 14
- “Configuring PPTP Internet Connectivity” on page 15

Tip: *If you do not know what kind of Internet connection you have, the **SonicWALL Setup Wizard** will attempt to detect your connection settings.*

Using the SonicWALL Setup Wizard

The SonicWALL **Setup Wizard** provides user-guided instructions for configuring your SonicWALL security appliance. If the **Setup Wizard** does not launch when you access the management interface, you can launch the **Setup Wizard** using one of the following methods:

- Select the **Network > Settings** and then click on the **Setup Wizard** button.
- Select the **System > Status** page and then click the **Wizards** button. The **SonicWALL Configuration Wizard** is displayed. Select **Setup Wizard** and click **Next**.
- Select **Wizards** on the left-navigation bar. The **SonicWALL Configuration Wizard** is displayed. Select **Setup Wizard** and click **Next**.

Note: *Make sure you have any required ISP information to complete the configuration before using the **Setup Wizard**.*

Tip: *You can also configure all your WAN and network settings on the **Network > Settings** page of the SonicWALL management interface.*

SonicWALL TZ 170 SP

If you are configuring the SonicWALL TZ 70 SP, the **Setup Wizard** includes two additional modem configuration pages for configuring the modem as the primary WAN connection or as a failover for the primary Internet connection. See “Configuring the TZ 170 SP using the Setup Wizard” on page 17.

SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless

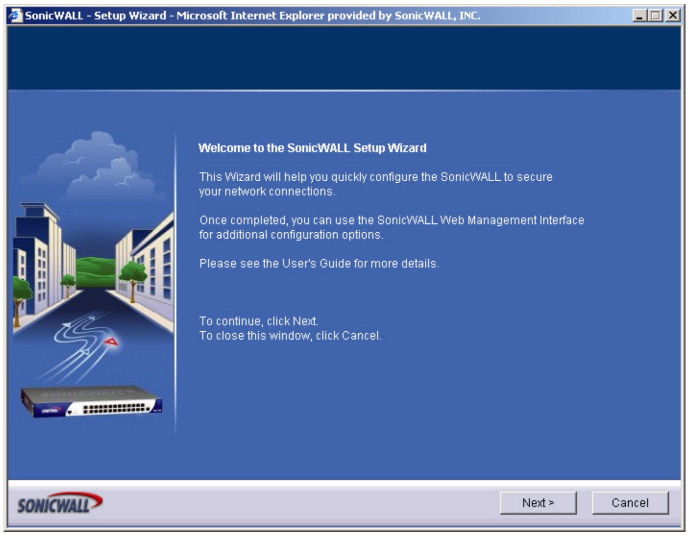
If you are configuring the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 70 Wireless, the **Setup Wizard** includes additional modem configuration pages for configuring the WLAN interface and setting up WiFISec security.

Configuring a Static IP Address Internet Connection

If you are assigned a single IP address by your ISP, perform the instructions below.

✓ : **Tip:** *Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.*

1 Click the **Setup Wizard** button on the **Network > Settings** page. The **Welcome to the SonicWALL Setup Wizard page** is displayed. Click **Next**.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

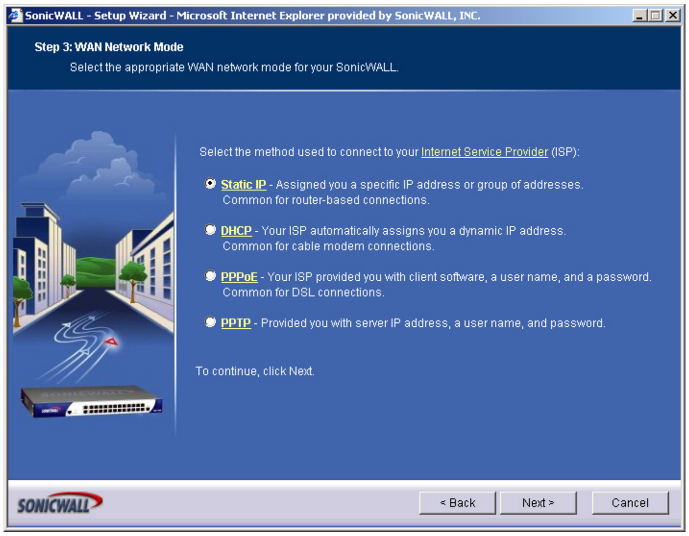
2 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next.**

Note: *Remember your password. You will need it to access the SonicWALL security appliance management interface after the initial configuration.*

3 Select your local time zone from the **Time Zone** menu. Click **Next**.

Note: *Set the time zone correctly before you register your SonicWALL security appliance.*

4 Choose **Static IP** and click **Next**.



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

● Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

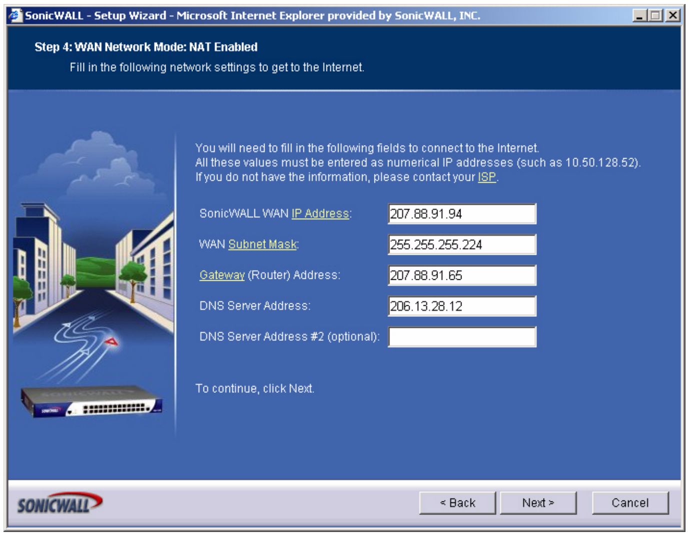
○ DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

○ PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

○ PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

5 Enter the information provided by your ISP in the following fields: **SonicWALL WAN IP Address**, **WAN Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next**.



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode: NAT Enabled

Fill in the following network settings to get to the Internet.

You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 10.50.128.52).
If you do not have the information, please contact your ISP.

SonicWALL WAN IP Address: 207.88.91.94
WAN Subnet Mask: 255.255.255.224
Gateway (Router) Address: 207.88.91.65
DNS Server Address: 206.13.28.12
DNS Server Address #2 (optional):

To continue, click Next.

6 The **LAN Settings** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask**. The **SonicWALL LAN IP Addresses** are the private IP address assigned to the LAN port of the SonicWALL security appliance. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL security appliance work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields.

7 Click **Next**. The **LAN DHCP Server** page configures the SonicWALL security appliance DHCP Server. If enabled, the SonicWALL security appliance automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

8 The **Configuration Summary** page displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to any previous page. If the configuration is correct, click **Apply**. The SonicWALL security appliance stores the network settings and then displays the **Setup Wizard Complete** page.

✓ **Tip:** *The SonicWALL security appliance LAN IP address, displayed in the* ***URL*** *field of the* ***Setup Wizard Complete*** *page, is used to log in and manage the SonicWALL security appliance.*

9. Click **Restart** to restart the SonicWALL security appliance. The SonicWALL security appliance takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

Configuring a DHCP Internet Connection

DHCP Internet connections are a common network configuration for customers with cable Internet service. You are not assigned a specific IP address by your ISP.

1. Click the **Setup Wizard** button on the **Network>Settings** page. The **Welcome to the SonicWALL Setup Wizard page** is displayed. Click **Next**.
2. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Note: *Remember your password. You will need it to access the SonicWALL security appliance management interface after the initial configuration.*

3. Select your local time zone from the **Time Zone** menu. Click **Next**.

Note: *Set the time zone correctly before you register your SonicWALL security appliance.*

4. Select **DHCP**. Click **Next**. A page is displayed describing an DHCP Internet connection.
5. Click **Next**.
6. The **LAN Settings** page allows the configuration of SonicWALL security appliance LAN IP Addresses and Subnet Masks. SonicWALL security appliance LAN IP Addresses are the private IP addresses assigned to the LAN of the SonicWALL security appliance. The **LAN Subnet Mask** defines the range of IP addresses on the networks. The default values provided by the SonicWALL security appliance are useful for most networks. Click **Next**.
7. The **LAN DHCP Server** window configures the SonicWALL security appliance DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses assigned to computers on the LAN.

   If **Disable DHCP Server** is selected, the DHCP Server is disabled. Click **Next** to continue.
8. The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to any previous page. If the configuration is correct, click **Apply**. The SonicWALL security appliance stores the network settings and then displays the **Setup Wizard Complete** page.

✓ **Tip:** *The new SonicWALL security appliance LAN IP address, displayed in the* ***URL*** *field of the* ***Setup Wizard Complete*** *page, is used to log in and manage the SonicWALL security appliance.*

9. Click **Restart** to restart the SonicWALL security appliance. The SonicWALL security appliance takes 90 seconds to restart. During this time, the yellow **Test** LED is lit.

Configuring a PPPoE Internet Connection

PPPoE is typically used for DSL Internet service using a DSL modem. The ISP requires a user name and password to log into the remote server.

1. Click the **Setup Wizard** button on the **Network > Settings** page. The **Welcome to the SonicWALL Setup Wizard page** is displayed. Click **Next**.
2. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

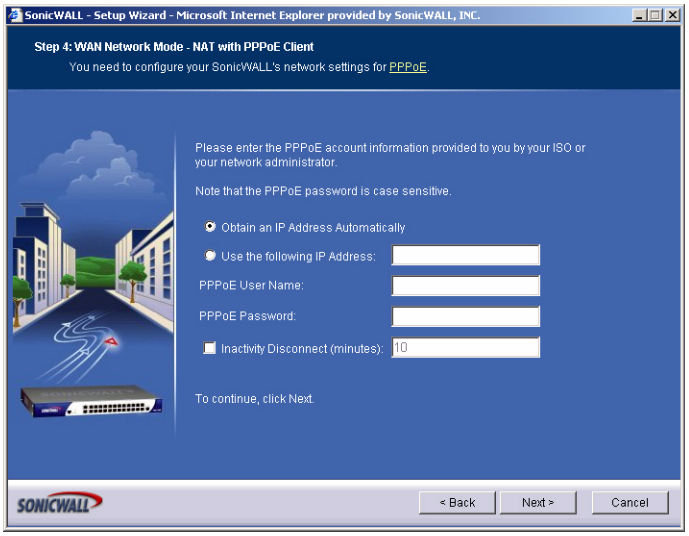
Note: *Remember your password. You will need it to access the SonicWALL security appliance management interface after the initial configuration.*

3 Select your local time zone from the **Time Zone** menu. Click **Next**.

Note: *Set the time zone correctly before you register your SonicWALL security appliance.*

4 Select **PPPoE**. Click **Next**.

5 Enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode - NAT with PPPoE Client

You need to configure your SonicWALL's network settings for PPPoE.

Please enter the PPPoE account information provided to you by your ISO or your network administrator.

Note that the PPPoE password is case sensitive.

● Obtain an IP Address Automatically

○ Use the following IP Address:

PPPoE User Name:

PPPoE Password:

☐ Inactivity Disconnect (minutes): 10

To continue, click Next.

6 The **LAN Settings** page allows the configuration of SonicWALL security appliance LAN IP Addresses and LAN Subnet Mask.The SonicWALL security appliance LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL security appliance. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL security appliance are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

7 The **LAN DHCP Server** window configures the SonicWALL security appliance DHCP Server. If enabled, the SonicWALL security appliance automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next.**

8 The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to any previous page. If the configuration is correct, click **Apply**. The SonicWALL security appliance stores the network settings and then displays the **Setup Wizard Complete** page.

✓ **Tip:** *The new SonicWALL security appliance LAN IP address, displayed in the* ***URL*** *field of the* ***Setup Wizard Complete*** *page, is used to log in and manage the SonicWALL security appliance.*

9 Click **Restart** to restart the SonicWALL security appliance. The SonicWALL security appliance takes 90 seconds to restart. During this time, the yellow **Test** LED is lit.

Configuring PPTP Internet Connectivity

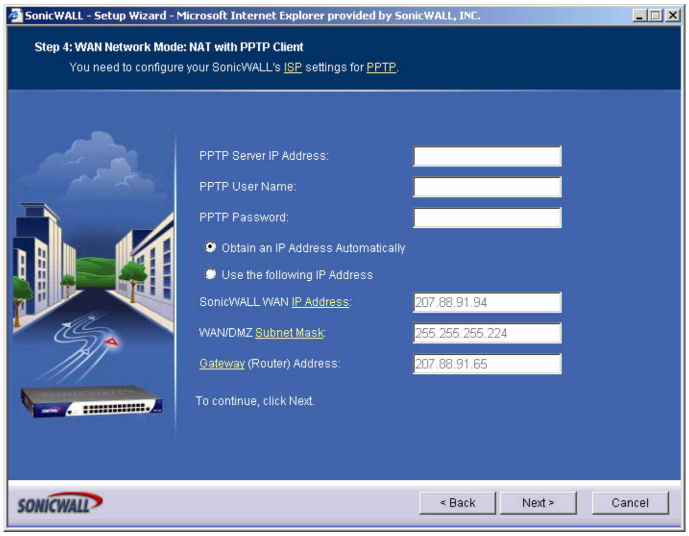
PPTP is used to connect to a remote server via an Internet connection. It supports older Microsoft implementations requiring tunneling connectivity.

1 Click the **Setup Wizard** button on the **Network > Settings** page. The **Welcome to the SonicWALL Setup Wizard page** is displayed. Click **Next**.

2 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

3 Select your local time from the **Time Zone** menu. Click **Next**.

4 Select **PPTP**. Click **Next**.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: WAN Network Mode: NAT with PPTP Client
You need to configure your SonicWALL's ISP settings for PPTP.

PPTP Server IP Address:
PPTP User Name:
PPTP Password:
● Obtain an IP Address Automatically
○ Use the following IP Address
SonicWALL WAN IP Address: 207.88.91.94
WAN/DMZ Subnet Mask: 255.255.255.224
Gateway (Router) Address: 207.88.91.65

To continue, click Next.

5 Enter the PPTP server IP address in the **PPTP Server IP Address** field.

6 Enter the user name and password provided by your ISP into the **PPTP User Name** and **PPTP Password** fields. Click **Next**.

7 The **LAN Settings** page allows the configuration of SonicWALL security appliance LAN IP Addresses and LAN Subnet Mask.The SonicWALL security appliance LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL security appliance. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL security appliance are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

8 The **LAN DHCP Server** window configures the SonicWALL security appliance DHCP Server. If enabled, the SonicWALL security appliance automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

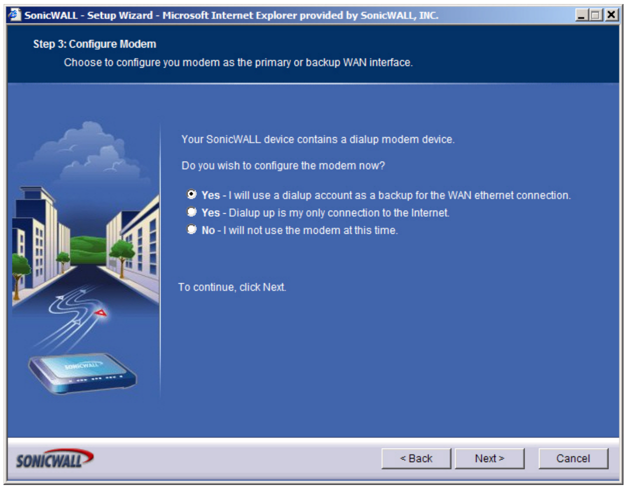
9 The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to any previous page. If the configuration is correct, click **Apply**. The SonicWALL security appliance stores the network settings and then displays the **Setup Wizard Complete** page.

✓ **Tip:** *The new SonicWALL security appliance LAN IP address, displayed in the* ***URL*** *field of the* ***Setup Wizard Complete*** *page, is used to log in and manage the SonicWALL security appliance.*

10 Click **Restart** to restart the SonicWALL security appliance. The SonicWALL security appliance takes 90 seconds to restart. During this time, the yellow **Test** LED is lit.

Configuring the TZ 170 SP using the Setup Wizard

Configuring the SonicWALL TZ 170 SP security appliance using the **Setup Wizard** includes two additional pages for configuring the SonicWALL TZ 170 SP's modem. Theses pages are displayed after the **Change Time Zone** page. Perform the following steps to configure the modem, and then return to the Setup Wizard instructions.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: Configure Modem

Choose to configure you modem as the primary or backup WAN interface.

Your SonicWALL device contains a dialup modem device.

Do you wish to configure the modem now?

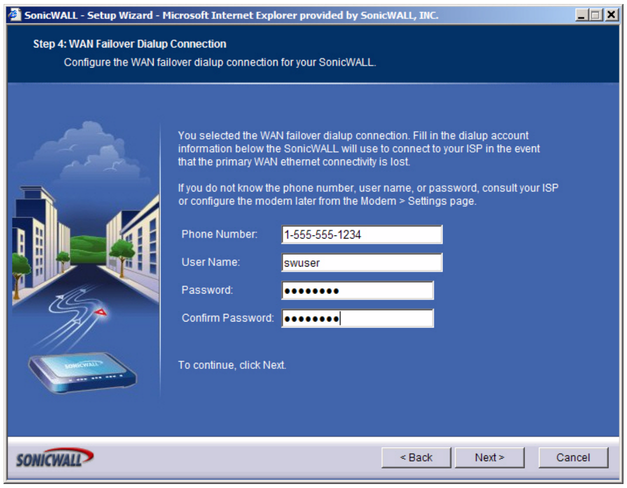
● **Yes** - I will use a dialup account as a backup for the WAN ethernet connection.
○ **Yes** - Dialup up is my only connection to the Internet.
○ **No** - I will not use the modem at this time.

To continue, click Next.

1 Select the way you will be using the built-in modem on the TZ 170 SP.

- **Yes - I will use a dialup account as a backup for the WAN ethernet connection**: This setting uses the modem dial-up connection as an automatic backup to the WAN ethernet connection. Use this if you have a DSL or Cable modem, and have dialup access to your ISP.
- **Yes - Dialup up is my only connection to the Internet**: This setting uses the modem dial-up connection as the only internet connection.
- **No - I will not use the modem at this time**: This setting does not use the modem.

2 Click **Next.**


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: WAN Failover Dialup Connection

Configure the WAN failover dialup connection for your SonicWALL.

You selected the WAN failover dialup connection. Fill in the dialup account information below the SonicWALL will use to connect to your ISP in the event that the primary WAN ethernet connectivity is lost.

If you do not know the phone number, user name, or password, consult your ISP or configure the modem later from the Modem > Settings page.

Phone Number: 1-555-555-1234
User Name: swuser
Password: ••••••••
Confirm Password: ••••••••

To continue, click Next.

3 If you selected to use the modem, enter the phone number, username and password for the dial-up connection. Click **Next**.

Configuring the TZ 50 Wireless/TZ 150 Wireless/170 Wireless using the Setup Wizard

The **Setup Wizard** provides the following four wireless deployment scenarios for the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless security appliances:

Office Gateway - Provides secure access for wired and wireless users on your network.

Secure Access Point - Add secure wireless access to an existing wireless network.

Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.

Secure Wireless Bridge - Operate in wireless bridge mode to securely bridge two networks with WiFiSec.

Configuring the TZ 50 Wireless/TZ 150 Wireless/170 Wireless as an Office Gateway

Log into the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless using your administrator's name and password. Click **Wizards** in the top right corner of the **System > Status** page.

Welcome to the SonicWALL Setup Wizard

1 To begin configuration, select **Setup Wizard** and click **Next**.

Selecting the Deployment Scenario

2 Select **Office Gateway** as the deployment scenario.

To view a description of each type of deployment scenario, click the name of the scenario.

Click **Next.**

Changing the Password

3 Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next.**

Selecting Your Time Zone

4 Select your Time Zone from the **Time Zone** menu. The security appliance uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode

5 Confirm that you have the proper network information necessary to configure the SonicWALL security appliance to access the Internet. Click the hyperlinks for definitions of the networking terms.

- You can choose:

•**Static IP**, if your ISP assigns you a specific IP address or group of addresses.

•**DHCP**, if your ISP automatically assigns you a dynamic IP address.

•**PPPoE**, if your ISP provided you with client software, a user name, and a password.

•**PPTP**, if your ISP provided you with a server IP address, a user name, and password.

6 Choose the correct networking mode and click **Next**.

Configuring WAN Settings

7 If you selected **Static IP address**, you must have your IP address information from your ISP to fill in the WAN Network Mode fields: Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address**, then fill in the rest of the fields: **WAN Subnet Mask**, **Gateway (Router) Address**, and the primary and secondary **DNS Server Addresses**. Click **Next**.

Configuring LAN Settings

8 Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field. The **Enable Windows Networking Support** checkbox is checked to allow Window networking support. If you do not want to allow Windows networking support, uncheck this setting. Click **Next**.

Configuring LAN DHCP Settings

9 If you want to use the SonicWALL security appliance’s DHCP Server, check the **Enable DHCP Server** on LAN checkbox and enter a range of IP addresses to assign network devices in the LAN **Address Range** fields. The default entries work for most network configurations. Click **Next**.

Configuring WLAN 802.11b/g Settings

10 The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Select a radio mode from the Radio Mode menu. The default **2.4GHz 802.11b/g Mixed** option allows the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support b and g. Select **United States - US** or **Canada - CA** from the **Country Code** menu. Use the default **AutoChannel** setting in the Channel menu. Click **Next**.

Configuring WiFiSec - VPN Client User Authentication

11 WiFiSec and GroupVPN are automatically enabled on the security appliance using the default settings associated with each feature. To add a user with VPN Client privileges, type a user name and password in the **User Name** and **Password** fields, and confirm your password in the **Confirm Password** field. When users access the security appliance using the VPN client, they are prompted for a user name and password. Click **Next**.

Configuring Wireless Guest Services

12 When **Enable Wireless Guest Services** is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

Configuration Summary

13 The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To use this configuration on the security appliance, click **Apply**.

Storing Configuration

14 Wait for the settings to take effect on the security appliance.

Congratulations

15 !When the settings are applied to the security appliance, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless as a Secure Access Point

Use the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless as a secure access point to add secure wireless access to an existing wireless network.

Log into the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless using your administrator's name and password. Click **Wizards** in the top right corner of the **System > Status** page.

Welcome to the SonicWALL Setup Wizard

1 To begin configuration, select **Setup Wizard** and click **Next**.

Selecting the Deployment Scenario

2 Select **Secure Access Point** as the deployment scenario. Click **Next**.

Changing the Password

3 Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone

4 Select your Time Zone from the **Time Zone** menu. The security appliance uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the LAN Settings

5 The **LAN** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask**.The **SonicWALL LAN IP Addresses** are the private IP address assigned to the LAN port of the SonicWALL security appliance. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL security appliance work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields. Fill in the **Gateway (Router) Address** and the primary and secondary **DNS Server Addresses**. Click **Next**.

Configuring the LAN DHCP Settings

6 The **LAN DHCP Settings** window configures the SonicWALL security appliance DHCP Server. If enabled, the SonicWALL security appliance automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server on LAN**, and specify the range of IP addresses that are assigned to computers on the LAN.

- If **Enable DHCP Server on LAN** is not selected, you must configure each computer on your LAN with a static IP address. Click **Next**.

Configuring WLAN 802.11b Settings

7 The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Select a radio mode from the Radio Mode menu. The default **2.4GHz 802.11b/g Mixed** option allows the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support b and g. Select **United States - US** or **Canada - CA** from the **Country Code** menu. Use the default **AutoChannel** setting in the Channel menu. Click **Next**.

Configuring WiFiSec - VPN Client User Authentication

8 WiFiSec and Group VPN are automatically enabled on the security appliance using the default settings associated with each feature. To add a user with VPN Client privileges, type a user name and password in the **User Name** and **Password** fields. When users access the security appliance using the VPN client, they are prompted for a user name and password. Click **Next**.

Configuration Summary

9 The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the security appliance, click **Apply**.

Storing Configuration

10 Wait for the settings to take effect on the security appliance.

Congratulations!

When the settings are applied to the security appliance, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless as a Guest Internet Gateway

Configure your wireless security appliance to provide guests controlled wireless access to the Internet only.

Log into the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless using your administrator’s name and password. Click **Wizards** in the top right corner of the **System > Status** page.

Welcome to the SonicWALL Setup Wizard

1 To begin configuration, select **Setup Wizard** and click **Next**.

Selecting the Deployment Scenario

2 Select **Guest Internet Gateway** as the deployment scenario. Click **Next**.

Changing the Password

3 Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone

4 Select your Time Zone from the **Time Zone** menu. The security appliance uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode

5 Confirm that you have the proper network information necessary to configure the SonicWALL security appliance to access the Internet. Click the hyperlinks for definitions of the networking terms.

You can choose:

- **Static IP**, if your ISP assigns you a specific IP address or group of addresses.
- **DHCP**, if your ISP automatically assigns you a dynamic IP address.

- **PPPoE**, if your ISP provided you with client software, a user name, and a password.
- **PPTP**, if your ISP provided you with a server IP address, a user name, and password.

6 Choose the correct networking mode and click **Next**.

Configuring WAN Settings

7 If you selected **Static IP address**, you must have your IP address information from your ISP to fill in the WAN Network Mode fields: Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address**, then fill in the rest of the fields: **WAN Subnet Mask**, **Gateway (Router) Address**, and the primary and secondary **DNS Server Addresses**. Click **Next**.

Configuring WLAN 802.11b Settings

8 The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Select a radio mode from the Radio Mode menu. The default **2.4GHz 802.11b/g Mixed** option allows the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support b and g. Select **United States - US** or **Canada - CA** from the **Country Code** menu. Use the default **AutoChannel** setting in the Channel menu. Click **Next.**

Configuring Wireless Guest Services

9 When Wireless Guest Services is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

Configuration Summary

10 The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the security appliance, click **Apply**.

Storing Configuration

11 Wait for the settings to take effect on the security appliance.

Congratulations!

When the settings are applied to the security appliance, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 170 Wireless as a Secure Wireless Bridge

Set up the TZ 170 Wireless as a Secure Wireless Bridge to securely bridge two networks with WiFiSec.

Log into the TZ 170 Wireless using your administrator’s name and password. Click **Wizards** in the top right corner of the **System > Status** page.

Welcome to the SonicWALL Setup Wizard

1 To begin configuration, select **Setup Wizard** and click **Next**.

Selecting the Deployment Scenario

2 Select **Secure Wireless Bridge** as the deployment scenario. Click **Next.**

Changing the Password

3 Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next.**

Selecting Your Time Zone

4 Select your Time Zone from the **Time Zone** menu. The security appliance uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring LAN Settings

5 Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field.

If you have Windows devices in both the LAN and WAN zones, you might want to enable windows networking between zones. However, this opens a potential security risk.

6 Click **Next**.

Configuring LAN DHCP Settings

7 If you want to use the security appliance's built-in DHCP server to assign dynamic IP Addresses within your LAN, check **Enable DHCP Server on LAN** and enter the range of addresses available to the DHCP Server. Click **Next**.

Configuring WLAN 802.11b Settings

8 The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Select a radio mode from the Radio Mode menu. The default **2.4GHz 802.11b/g Mixed** option allows the SonicWALL TZ 170 Wireless to support b and g. Select **United States - US** or **Canada - CA** from the **Country Code** menu. Use the default **AutoChannel** setting in the Channel menu. Click **Next.**

Configuring WLAN Network Setting

9 Enter the appropriate network configuration for the security appliance to work in your bridged network environment. Type a private IP address in the **SonicWALL WLAN IP Address** field. Type the subnet in the **Subnet Mask** field. Enter that address of the **Gateway (Router) Address** and the **DNS Server Address**. If you have a secondary DNS server you can enter its address.

10 Click **Next.**

Configuring Secure Wireless Bridge Settings

Complete the VPN Security Policy information to configure the Secure Wireless Bridge. Enter the VPN **Policy Name**, the Peer **IPSec Gateway Address**, and the IKE **Shared Secret**. Click **Next** to continue.

Configuration Summary

11 The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the security appliance, click **Apply**.

Storing Configuration

12 Wait for the settings to take effect on the security appliance.

Congratulations!

When the settings are applied to the security appliance, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Registering Your SonicWALL Security Appliance

Once you have established your Internet connection, it is recommended you register your SonicWALL security appliance. Registering your SonicWALL security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus, Content Filtering Service, and Network Anti-Virus.
- Activate SonicWALL security services and upgrades
- Access SonicOS firmware updates
- Get SonicWALL technical support

Before You Register

If your SonicWALL security appliance is not registered, the following message is displayed in the **Security Services** folder on the **System > Status** page in the SonicWALL management interface: **Your SonicWALL is not registered. Click here to Register your SonicWALL**. You need a mySonicWALL.com account to register the SonicWALL security appliance.

If your SonicWALL security appliance is connected to the Internet, you can create a mySonicWALL.com account and register your SonicWALL security appliance directly from the SonicWALL management interface. If you already have a mySonicWALL.com account, you can register the SonicWALL security appliance directly from the management interface.

Your mySonicWALL.com account is accessible from any Internet connection by pointing your Web browser to *<https://www.mysonicwall.com>.* mySonicWALL.com uses the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.

Alert: *Make sure the **Time Zone** and **DNS** settings on your SonicWALL security appliance are correct when you register the device. See SonicWALL Setup Wizard instructions for instructions on using the **Setup Wizard** to set the **Time Zone** and **DNS** settings.*

Note: *mySonicWALL.com registration information is not sold or shared with any other company.*

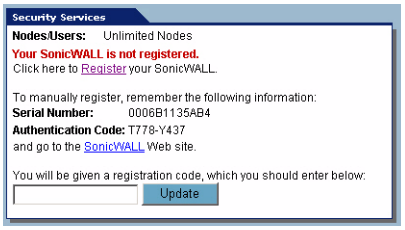
You can also register your security appliance at the *<https://www.mysonicwall.com>* site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **SonicWALL** link to access your mySonicWALL.com account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL management interface.

To create a mySonicWALL.com account from the SonicWALL management interface:

1 In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**.

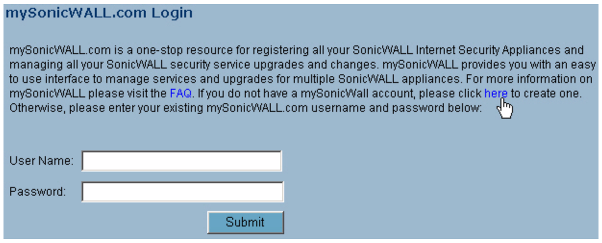


Nodes/Users: Unlimited Nodes
Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B1135AB4
Authentication Code: T778-Y437
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

2 Click the **here** link in **If you do not have a mySonicWALL account, please click here to create one** on the **mySonicWALL Login** page.



mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:
Password:

3 In the **MySonicWALL Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields in the mySonicWALL.com account form. All fields marked with an ***** are required fields.

Note: *Remember your username and password to access your mySonicWALL.com account.*

4 Click **Submit** after completing the **MySonicWALL Account** form.

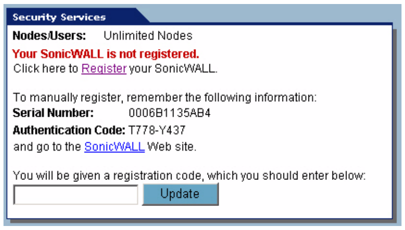
5 When the mySonicWALL.com server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.

6 Congratulations! Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com from the management appliance to register your SonicWALL security appliance.

Registering Your SonicWALL Security Appliance

If you already have a mySonicWALL.com account, follow these steps to register your security appliance:

1 In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**. The **mySonicWALL Login** page is displayed.



Nodes/Users: Unlimited Nodes
Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B1135AB4
Authentication Code: T778-Y437
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

2 In the **mySonicWALL.com Login** page, enter your mySonicWALL.com username and password in the **User Name** and **Password** fields and click **Submit**.

3 The next several pages inform you about free trials available to you for SonicWALL's Security Services:

- **Gateway Anti-Virus -** protects your entire network from viruses

- **Network Anti-Virus** - protects computers on your network from viruses
- **Premium Content Filtering Service -** protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
- **Intrusion Prevention Service -** protects your network from Trojans, worms, and application layer attacks.

Click **Continue** on each page.

4 At the top of the Product Survey page, enter a friendly name for your SonicWALL security appliance in the **Friendly name** field, and complete the optional product survey.

5 Click **Submit**.

6 When the mySonicWALL.com server has finished processing your registration, a page is displayed confirming your SonicWALL security appliance is registered.

7 Click **Continue**. The **Manage Services Online** table on the **System > Licenses** page displayed.

Cross Reference: *Refer to Part 7, Security Services for information on SonicWALL security services and activating FREE trials.*

PART

2

System

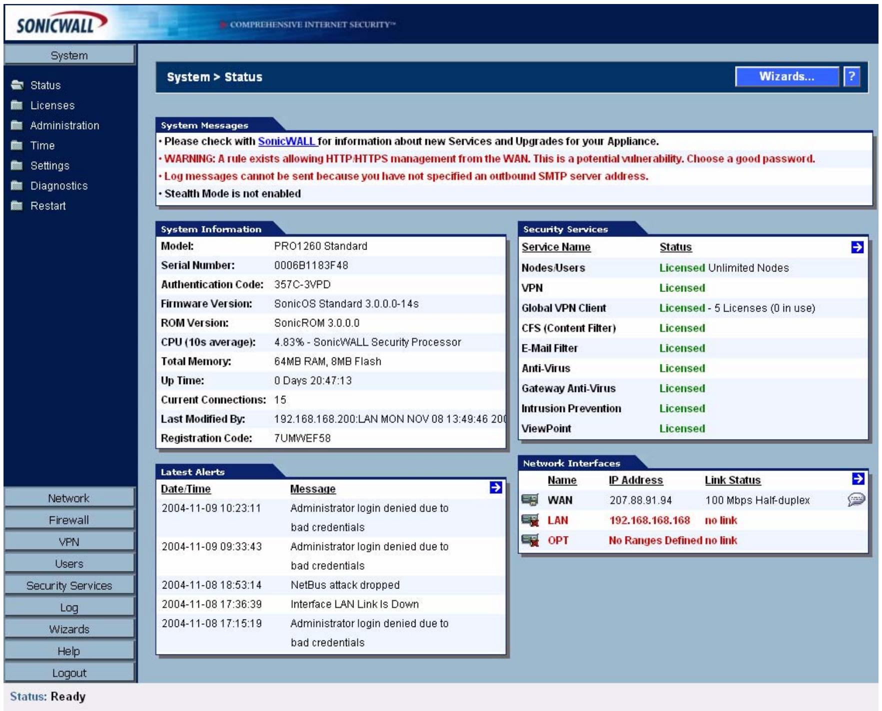
C H A P T E R

3

Viewing System Status Information

System > Status

The **Status** page contains five sections: **System Messages, System Information, Latest Alerts, Security Services,** and **Network Interfaces**.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
System > Status
Wizards...
?
Status: Ready

System Messages

- Please check with SonicWALL for information about new Services and Upgrades for your Appliance.
- WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- Stealth Mode is not enabled

System Information

Model:	PRO1260 Standard
Serial Number:	0006B1183F48
Authentication Code:	357C-3VPD
Firmware Version:	SonicOS Standard 3.0.0.0-14s
ROM Version:	SonicROM 3.0.0.0
CPU (10s average):	4.83% - SonicWALL Security Processor
Total Memory:	64MB RAM, 8MB Flash
Up Time:	0 Days 20:47:13
Current Connections:	15
Last Modified By:	192.168.168.200:LAN MON NOV 08 13:49:46 200
Registration Code:	7UMWEF58

Security Services

Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 5 Licenses (0 in use)
CFS (Content Filter)	Licensed
E-Mail Filter	Licensed
Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Intrusion Prevention	Licensed
ViewPoint	Licensed

Latest Alerts

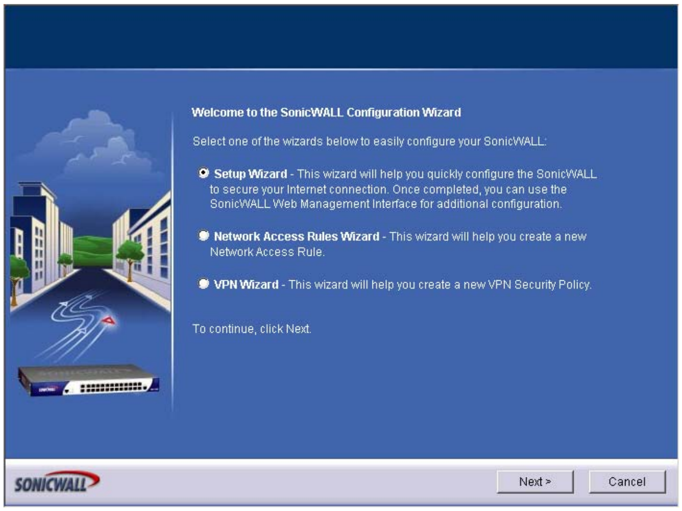
Date/Time	Message
2004-11-09 10:23:11	Administrator login denied due to bad credentials
2004-11-09 09:33:43	Administrator login denied due to bad credentials
2004-11-08 18:53:14	NetBus attack dropped
2004-11-08 17:36:39	Interface LAN Link Is Down
2004-11-08 17:15:19	Administrator login denied due to bad credentials

Network Interfaces

Name	IP Address	Link Status
WAN	207.88.91.94	100 Mbps Half-duplex
LAN	192.168.168.168	no link
OPT	No Ranges Defined	no link

Wizards

The **Wizards** button on the **System > Status** page provides access to the **SonicWALL Configuration Wizard**.



Welcome to the SonicWALL Configuration Wizard

Select one of the wizards below to easily configure your SonicWALL:

● **Setup Wizard** - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.

○ **Network Access Rules Wizard** - This wizard will help you create a new Network Access Rule.

○ **VPN Wizard** - This wizard will help you create a new VPN Security Policy.

To continue, click Next.

This wizard allows you to easily configure the SonicWALL security appliance using the following wizards:

- **Setup Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to secure your Internet (WAN) and LAN connections.
- **Network Access Rules Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to provide public access to an internal server, such as a Web or E-mail server or create a general firewall rule.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWALL Global VPN Clients.

System Messages

Any information considered relating to possible problems with configurations on the SonicWALL security appliance such as password, log messages, etc.

System Information

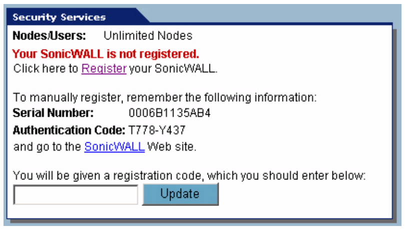
The following information is displayed in this section:

- **Model** - type of SonicWALL security appliance
- **Serial Number** - also the MAC address of the SonicWALL security appliance
- **Authentication Code** - the alphanumeric code used to authenticate the SonicWALL security appliance on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - the firmware version loaded on the SonicWALL security appliance.
- **ROM Version** - indicates the ROM version.
- **CPU** - displays the percent usage and the type of the SonicWALL security appliance processor.
- **Total Memory** - indicates the amount of RAM and flash memory.
- **Up Time** - the length of time, in days, hours, minutes, and seconds the SonicWALL security appliance is active.
- **Current Connections** - the number of network connections currently existing on the SonicWALL security appliance.
- **Last Modified By**- the IP address the administrator connected from and the time of the last modification.

- **Registration Code** - the registration code is generated when your SonicWALL security appliance is registered at <https://www.mysonicwall.com>.

Security Services

If your SonicWALL security appliance is not registered at mySonicWALL.com, the following message is displayed in the **Security Services** folder: **Your SonicWALL security appliance is not registered. Click here to Register your SonicWALL** security appliance. You need a mySonicWALL.com account to register your SonicWALL security appliance or activate security services. You can create a mySonicWALL.com account directly from the SonicWALL management interface.



Nodes/Users: Unlimited Nodes

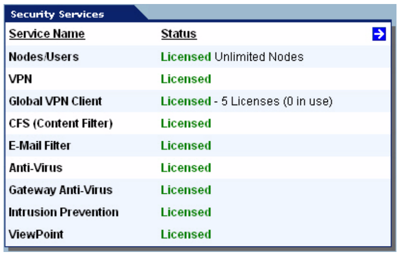
Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B1135AB4
Authentication Code: T778-Y437
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

Cross Reference: *Refer to **Chapter 2, Basic SonicWALL Security Appliance Setup** for complete registration instructions.*

If your SonicWALL security appliance is registered a list of available SonicWALL Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Arrow** icon displays the **System > Licenses** page in the SonicWALL Web-based management interface. SonicWALL Security Services and SonicWALL security appliance registration is managed by mySonicWALL.com.



Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 5 Licenses (0 in use)
CFS (Content Filter)	Licensed
E-Mail Filter	Licensed
Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Intrusion Prevention	Licensed
ViewPoint	Licensed

Cross Reference: *Refer to Part 7, Security Services for more information on SonicWALL Security Services and activating them on the SonicWALL security appliance.*

Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the **Log > Log View** page.

Network Interfaces

The Network Interfaces displays the IP address and link information for interfaces on your SonicWALL security appliance. The available interfaces displayed in this section depends on the SonicWALL security appliance model. Clicking the arrow displays the **Network > Settings** page.

SonicWALL Security Appliance Model	**Interfaces**
SonicWALL TZ 50	**WAN**, **LAN**
SonicWALL TZ 50 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL TZ 150	**WAN**, **LAN**
SonicWALL TZ 150 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL TZ 170	**WAN**, **LAN**, **OPT**
SonicWALL TZ 170 SP	**WAN**, **LAN**, **Modem**
SonicWALL TZ 170 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL PRO 1260	**WAN**, **LAN**, **OPT**
SonicWALL PRO 2040	**WAN, LAN, DMZ**
SonicWALL PRO 3060	**WAN**, **LAN**, **DMZ**

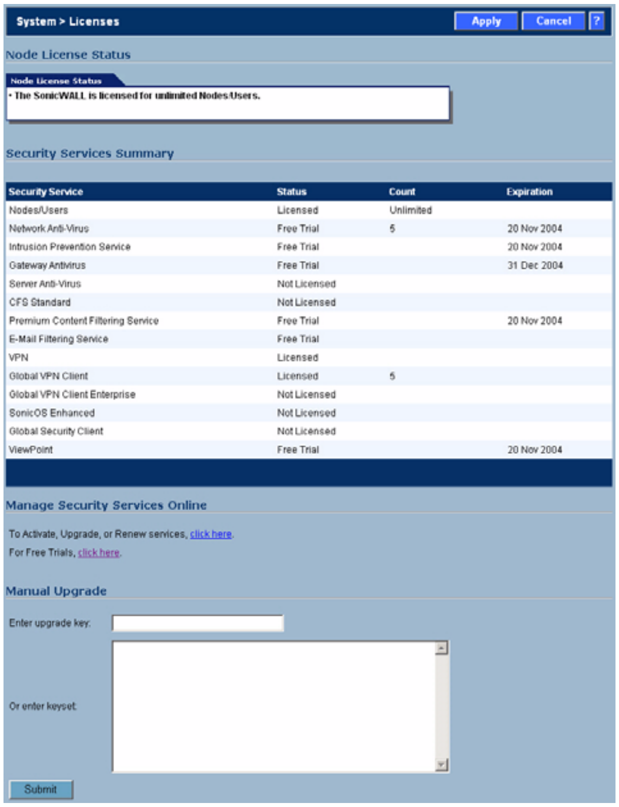
➲ **Cross Reference:** *Refer to **Chapter 9, Configuring Network Settings** for more information on configuring Network Interfaces.*

CHAPTER 4

System > Licenses

System > Licenses

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services and upgrades.



Node License Status

Node License Status

- The SonicWALL is licensed for unlimited Nodes/Users.

Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
Network Anti-Virus	Free Trial	5	20 Nov 2004
Intrusion Prevention Service	Free Trial		20 Nov 2004
Gateway Antivirus	Free Trial		31 Dec 2004
Server Anti-Virus	Not Licensed		
CFS Standard	Not Licensed		
Premium Content Filtering Service	Free Trial		20 Nov 2004
E-Mail Filtering Service	Free Trial		
VPN	Licensed		
Global VPN Client	Licensed	5	
Global VPN Client Enterprise	Not Licensed		
SonicOS Enhanced	Not Licensed		
Global Security Client	Not Licensed		
ViewPoint	Free Trial		20 Nov 2004

Manage Security Services Online

To Activate, Upgrade, or Renew services, click here.

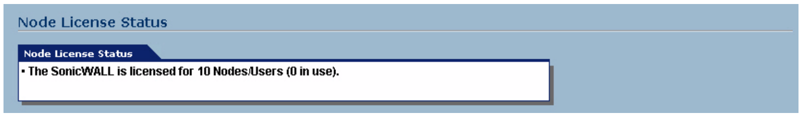
For Free Trials, click here.

Manual Upgrade

Enter upgrade key:

Or enter keyset:

Node License Status

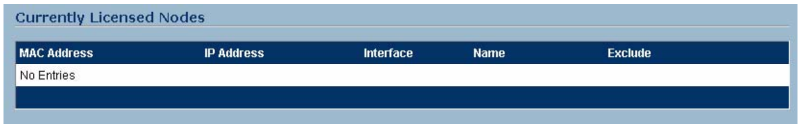

Node License Status
Node License Status

• The SonicWALL is licensed for 10 Nodes/Users (0 in use).

Node licensing can be monitored and controlled from the **System > Licenses** page. The **Node License Status** section displays the number of licensed nodes, and the number of nodes currently in use. To prevent nodes from consuming licenses (such as for network printers that do not require Internet access) a facility is provided to construct an exclusion list.

If your SonicWALL security appliance supports an unlimited number of nodes, the **Node License Status** section does not include **Currently Licensed Nodes** and **Node License Exclusion List** settings.

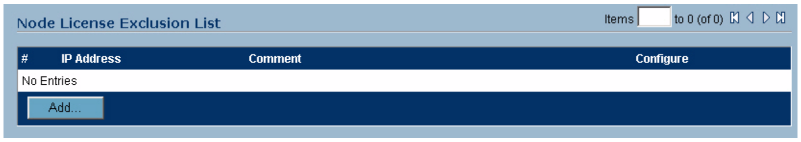
Currently Licensed Nodes


Currently Licensed Nodes
MAC Address
IP Address
Interface
Name
Exclude
No Entries

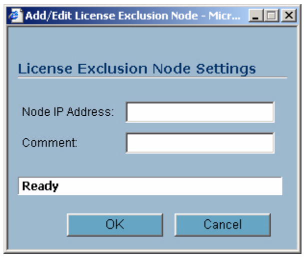
On node restricted devices, node usage is calculated by the number of active hosts on local interfaces attempting to traverse the WAN interface. After a 5 minute period of inactivity, hosts are no longer considered active, and are removed from the **Currently Licensed Nodes** list. Subsequent activity will add them back to the list.

When the node license limit has been reached, an over-limit host will be denied access to the WAN, and if the traffic the host is attempting is HTTP, the host is redirected to the License Exceed page on the SonicWALL security appliance.

Node License Exclusion List


Node License Exclusion List
Items
to 0 (of 0)
#
IP Address
Comment
Configure
No Entries
Add...

IP Addresses can be added to the **Node License Exclusion List** by clicking the **Add** button. The **Add/Edit License Exclusion Node** window is displayed.


Add/Edit License Exclusion Node - Micr...
License Exclusion Node Settings
Node IP Address:
Comment:
Ready
OK
Cancel

Enter the node IP address in the **Node IP Address** field and an optional comment in the **Comment** field.

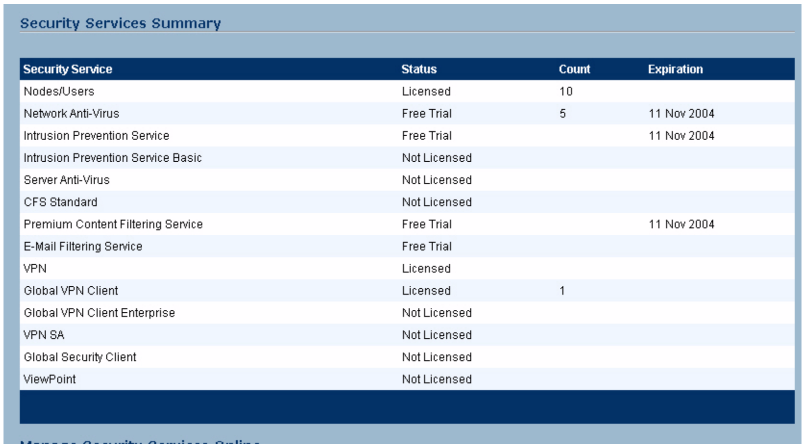
You can clicking on the icon in the **Exclude** column of the **Currently Licensed Nodes** table to automatically add the entry to the **Node License Exclusion List**. Clicking the icon displays an alert explaining that the host to be excluded and added to the exclusion list, and the node will be prohibited from accessing the WAN. Clicking **OK**. The **Node License Exclusion List** is updated to reflect the change.

The delete icon can be used to remove entries from the list, and to restore WAN access to the referenced host. The edit icon allows for a comment to be added or changed on the entry.

The **Node License Exclusion List** table is also be updated to reflect the change:

Clicking the **Auto Firewall Access Rule** redirects the management session to the **Firewall > Access** Rules page, where the auto-created, non-editable rule can be viewed.

Security Services Summary



Security Services Summary

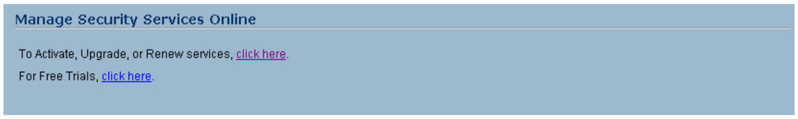
Security Service	Status	Count	Expiration
Nodes/Users	Licensed	10	
Network Anti-Virus	Free Trial	5	11 Nov 2004
Intrusion Prevention Service	Free Trial		11 Nov 2004
Intrusion Prevention Service Basic	Not Licensed		
Server Anti-Virus	Not Licensed		
CFS Standard	Not Licensed		
Premium Content Filtering Service	Free Trial		11 Nov 2004
E-Mail Filtering Service	Free Trial		
VPN	Licensed		
Global VPN Client	Licensed	1	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Not Licensed		
Global Security Client	Not Licensed		
ViewPoint	Not Licensed		

The **Security Services Summary** table lists the available and activated security services on the SonicWALL security appliance. The Security Service column lists all the available SonicWALL security services and upgrades available for the SonicWALL security appliance. The **Status** column indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column.

The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account the next time the SonicWALL security appliance automatically synchronizes with your mySonicWALL.com account (once a day) or you can click the link in **To synchronize licenses with mySonicWALL.com click here** in the **Manage Security Services Online** section.

Note: *Refer to Chapter 8, Setting Up Security Services for more information on SonicWALL Security Services and activating them on the SonicWALL security appliance.*

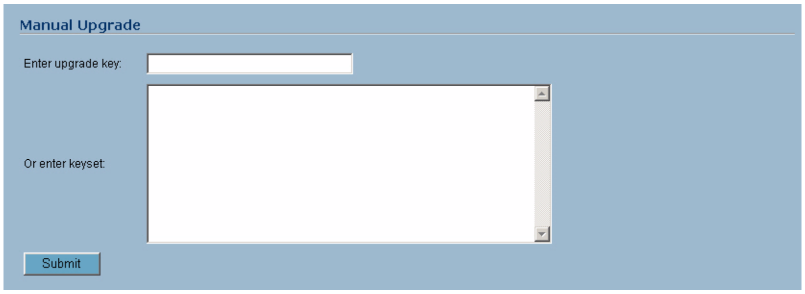
Manage Security Services Online


Manage Security Services Online
To Activate, Upgrade, or Renew services, click here.
For Free Trials, click here.

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with mySonicWALL.com click here** to synchronize your mySonicWALL.com account with the **Security Services Summary** table.

You can also get free trial subscriptions to SonicWALL Content Filter Service and Network Anti-Virus by clicking the **For Free Trials click here link**. When you click these links, the **mySonicWALL.com Login** page is displayed. Enter your mySonicWALL.com account username and password in the **User Name** and Password fields and click Submit. The **Manage Services Online** page is displayed with licensing information from your mySonicWALL.com account.

Manual Upgrade



Manual Upgrade allows you to activate your services by typing the service activation key supplied with the service subscription not activated on mySonicWALL.com. Type the activation key from the product into the **Enter upgrade key** field and click **Submit**.

✓ **Tip:** *You must have a mysonicwall.com account to upgrade and activate services through the SonicWALL security appliance.*

Manual Upgrade for Closed Environments

If your SonicWALL security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWALL security appliance, you can enter the encrypted license key information from http://www.mysonicwall.com manually on the **System > Licenses** page in the SonicWALL Management Interface.

Note: *Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your SonicWALL security appliance.*

From a Computer Connected to the Internet

1. Make sure you have an account at http://www.mysonicwall.com and your SonicWALL security appliance is registered to the account before proceeding.
2. After logging into www.mysonicwall.com, click on your registered SonicWALL security appliance listed in **Registered SonicWALL Products**.
3. Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWALL security appliance and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWALL security appliance.

From the Management Interface of the SonicWALL Security Appliance

4. Make sure your SonicWALL security appliance is running SonicOS Standard or Enhanced 2.1 (or higher).
5. Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page (SonicOS).
6. Click the **Submit** or the **Apply** button to update your SonicWALL security appliance. The status field at the bottom of the page displays The configuration has been updated.
7. You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.

After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information. The warning message: **SonicWALL Registration Update Needed. Please update your registration information** remains on the **System > Status** page after you have registered your SonicWALL security appliance. Ignore this message.

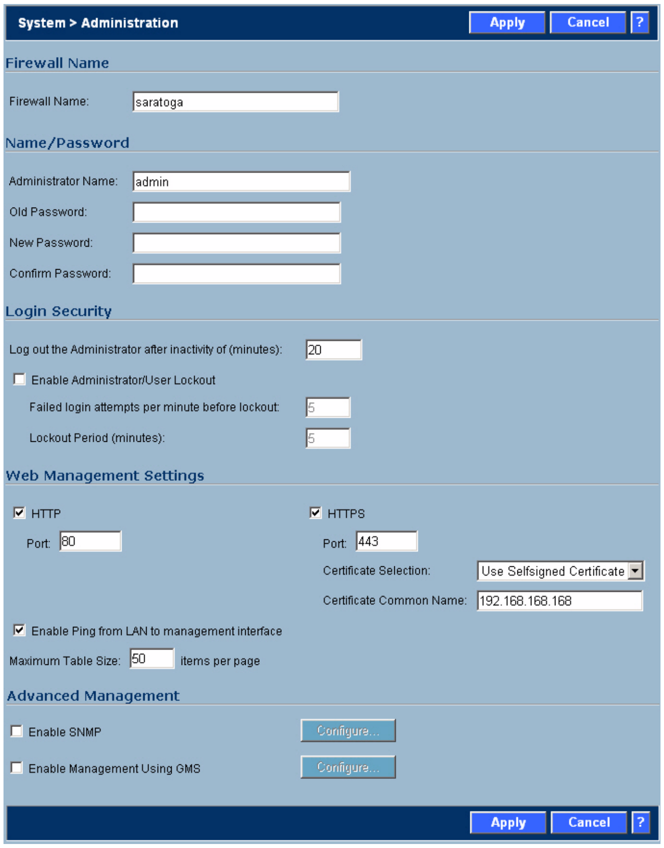
CHAPTER

5

Using System Administration

System > Administration

The **System > Administration** page provides settings for the configuration of SonicWALL security appliance for secure and remote management. You can manage the SonicWALL security appliance using a variety of methods, including HTTPS, SNMP or SonicWALL Global Management System (SonicWALL GMS).



Firewall Name

Firewall Name: saratoga

Name/Password

Administrator Name: admin

Old Password:

New Password:

Confirm Password:

Login Security

Log out the Administrator after inactivity of (minutes): 20

☐ Enable Administrator/User Lockout

Failed login attempts per minute before lockout: 5

Lockout Period (minutes): 5

Web Management Settings

☑ HTTP

Port: 80

☑ HTTPS

Port: 443

Certificate Selection: Use Selfsigned Certificate

Certificate Common Name: 192.168.168.168

☑ Enable Ping from LAN to management interface

Maximum Table Size: 50 items per page

Advanced Management

☐ Enable SNMP

☐ Enable Management Using GMS

Firewall Name

The **Firewall Name** uniquely identifies the SonicWALL security appliance and defaults to the serial number of the SonicWALL security appliance. The serial number is also the MAC address of the unit. The Firewall Name is mainly used in e-mailed log files. To change the Firewall Name, enter a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

Name/Password

Administrator Name

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create an new administrator name, enter the new name in the **Administrator Name** field. Click **Apply** for the changes to take effect on the SonicWALL security appliance.

Changing the Administrator Password

To set the password, enter the old password in the **Old Password** field, and the new password in the **New Password** field. Enter the new password again in the **Confirm New Password** field and click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

Login Security

The **Log out the Administrator after inactivity of (minutes)** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the management interface. By default, the SonicWALL security appliance logs out the administrator after 5 minutes of inactivity.

Tip: *If the **Administrator Inactivity Timeout** is extended beyond 5 minutes, you should end every management session by clicking **Logout** to prevent unauthorized access to the SonicWALL Web Management Interface.*

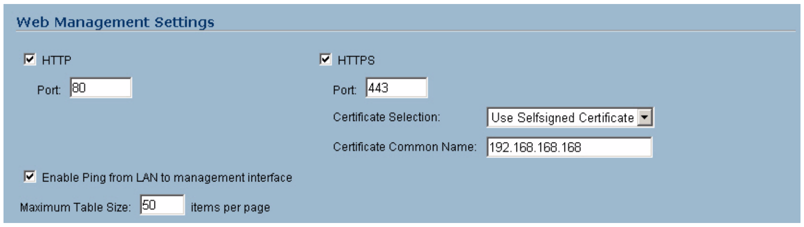
Enter the desired number of minutes in the **Log out the Administrator after inactivity of (minutes)** setting and click **Apply**. The time range can be from 1 to 99 minutes. Click **Apply**, and a message confirming the update is displayed at the bottom of the browser window.

Enable Administrator/User Lockout

You can configure the SonicWALL security appliance to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout** check box to prevent users from attempting to log into the SonicWALL security appliance without proper authentication credentials. Enter the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field. Enter the length of time that must elapse before the user attempts to log into the SonicWALL security appliance again in the **Lockout Period (minutes)** field.

Alert: *If the administrator and a user are logging into the SonicWALL security appliance using the same source IP address, the administrator is also locked out of the SonicWALL security appliance. The lockout is based on the source IP address of the user or administrator.*

Web Management Settings



Web Management Settings

☑ HTTP

Port: 80

☑ HTTPS

Port: 443

Certificate Selection: Use Selfsigned Certificate

Certificate Common Name: 192.168.168.168

☑ Enable Ping from LAN to management interface

Maximum Table Size: 50 items per page

The SonicWALL security appliance can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Enter the number of the desired port in the **Port** field, and click **Update**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security appliance. For example, if you configure the port to be 76, then you must enter <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>

The default port for HTTPS management is 443, the standard port. You can add another layer of security for logging into the SonicWALL security appliance by changing the default port. To configure another port for HTTPS management, enter the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWALL security appliance using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the SonicWALL security appliance.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL security appliance. You can also choose **Import Certificate** to select an imported certificate from the **VPN > Local Certificates** page to use for authentication to the Management Interface.

The **Enable Ping from LAN to management interface** setting allows a LAN user to ping the SonicWALL to verify it is online.

Changing the Default Size for SonicWALL Management Interface Tables

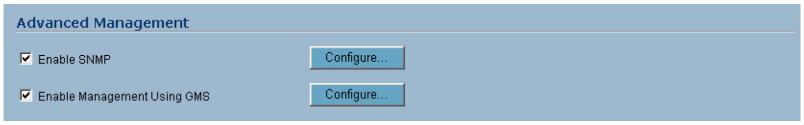
The SonicWALL Management Interface allows you to control the display of large tables of information across all tables in the management Interface; for example the table on the **Firewall > Access Rules** page.

You can change the default table page size in all tables displayed in the SonicWALL Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items.

To change the default table size:

1. Enter the maximum table size number in the **Table Size** field.
2. Click **Apply**.

Advanced Management



Advanced Management

☑ Enable SNMP

☑ Enable Management Using GMS

Enable SNMP

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL security appliance and receive notification of critical events as they occur on the network. The SonicWALL security appliance supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The SonicWALL security appliance replies to SNMP Get commands for MIBII via any interface and supports a custom SonicWALL MIB for generating trap messages. The custom SonicWALL MIB is available for download from the SonicWALL Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

To enable SNMP on the SonicWALL security appliance, select the **Enable SNMP** check box, and then click **Configure** in the **System > Administration** page.

Note: *v1 traps are not supported on the SonicWALL security appliance.*

1. Enter the host name of the SonicWALL security appliance in the **System Name** field.
2. Enter the network administrator’s name in the **System Contact** field.
3. Enter an e-mail address, telephone number, or pager number in the **System Location** field.
4. Enter a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
5. Enter a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
6. Enter the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
7. Click **OK**.

Trap messages are generated only for the alert message categories normally sent by the SonicWALL security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log > Settings** page, then no trap messages are generated.

By default, the SonicWALL security appliance responds only to **Get SNMP** messages received on its LAN interface. Appropriate rules must be configured to allow SNMP traffic to and from the WAN interface. SNMP trap messages can be sent via the LAN or WAN.

Note: *Refer to Chapter 4, Configuring Firewall Settings for instructions on adding services and rules to the SonicWALL security appliance.*

If your SNMP management system supports discovery, the SonicWALL agent automatically discover the SonicWALL security appliance on the network. Otherwise, you must add the SonicWALL security appliance to the list of SNMP-managed devices on the SNMP management system.

Enable Management Using SonicWALL GMS

To enable the SonicWALL security appliance to be managed by SonicWALL Global Management System (GMS). Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.

To configure the SonicWALL security appliance for GMS management:

1. Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
2. Enter the port in the **GMS Syslog Server Port** field. The default value is 514.
3. Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
4. Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
5. Select one of the following GMS modes from the **Management Mode** menu.

   IPSEC Management Tunnel - Use the IPSec management tunnel included with the SonicWALL security appliance. The default IPSec VPN settings are displayed.

   Existing Tunnel - Use an existing tunnel for GMS management of the SonicWALL security appliance.

   HTTPS - Use HTTPS for GMS management of the SonicWALL security appliance. The following configuration settings for HTTPS management mode are displayed:

      Send Syslog Messages in Cleartext Format - Sends Syslog messages as cleartext.

      Send Syslog Messages to a Distributed GMS Reporting Server - Sends Syslog Messages to a GMS Reporting Server separated from the GMS management server.

      GMS Reporting Server IP Address - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.

      GMS Reporting Server Port - Enter the port for the GMS Reporting Server. The default value is 514

6. Click **OK**.

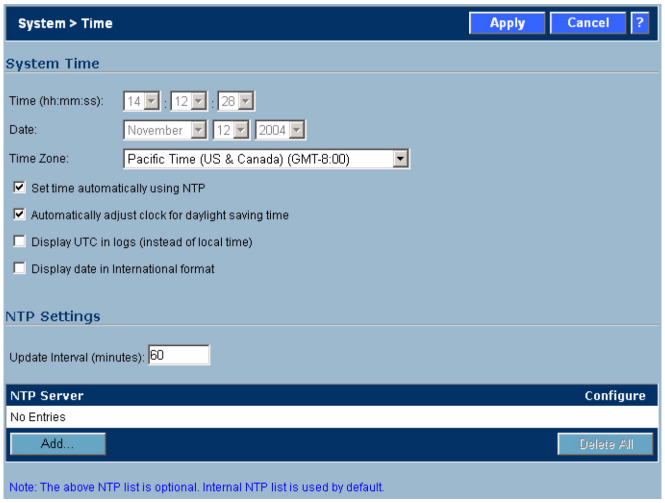
CHAPTER

6

Setting System Time

System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes.



System Time

Time (hh:mm:ss): 14 : 12 : 28

Date: November 12 2004

Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Set time automatically using NTP

☑ Automatically adjust clock for daylight saving time

☐ Display UTC in logs (instead of local time)

☐ Display date in International format

NTP Settings

Update Interval (minutes): 60

NTP Server	Configure
No Entries	

Note: The above NTP list is optional. Internal NTP list is used by default.

By default, the SonicWALL security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Set Time

The SonicWALL security appliance uses the time and date settings to time stamp log events, to automatically update filtering subscription services, and for other internal purposes. By default, the SonicWALL security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Setting the SonicWALL Security Appliance Time

To select your time zone and automatically update the time, choose the time zone from the **Time Zone** menu. The **Set time automatically using NTP** setting is activated by default to use the NTP (Network Time Protocol) to set time automatically. If you want to set your time manually, uncheck this setting. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus. **Automatically adjust clock for daylight saving changes** is activated by default to enable automatic adjustments for daylight savings time.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display time in International format** displays the date in International format, with the day preceding the month.

After selecting your system time settings, click **Apply**.

NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond. The SonicWALL security appliance use an internal list of NTP servers so manually entering a NTP server is optional.

Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL security appliance clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL security appliance. The default value is 60 minutes.

To add an NTP server to the SonicWALL security appliance configuration, click **Add**. The **Add NTP Server** window is displayed. Type the IP address of an NTP server in the **NTP Server** field. Click **Ok**. Then click **Apply** on the **System > Time** page to update the SonicWALL security appliance. To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.

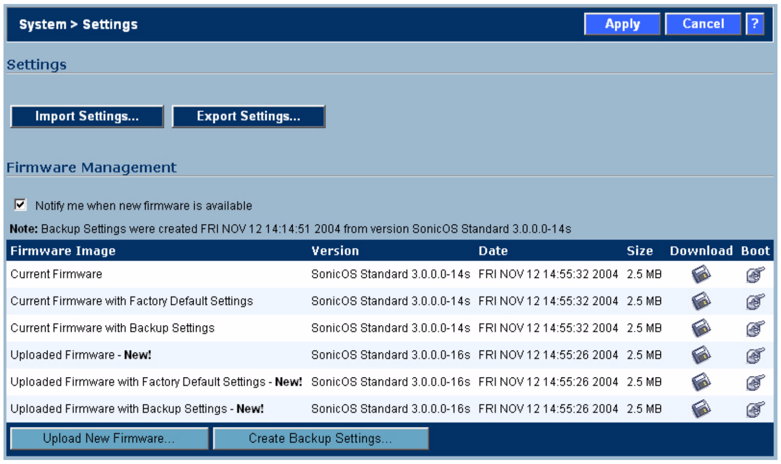
CHAPTER

7

Configuring System Settings

System > Settings

The **System > Settings** page includes features for managing the SonicWALL security appliance firmware and your custom preferences.



☑ Notify me when new firmware is available

Note: Backup Settings were created FRI NOV 12 14:14:51 2004 from version SonicOS Standard 3.0.0.0-14s

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Standard 3.0.0.0-14s	FRI NOV 12 14:55:32 2004	2.5 MB		
Current Firmware with Factory Default Settings	SonicOS Standard 3.0.0.0-14s	FRI NOV 12 14:55:32 2004	2.5 MB		
Current Firmware with Backup Settings	SonicOS Standard 3.0.0.0-14s	FRI NOV 12 14:55:32 2004	2.5 MB		
Uploaded Firmware - **New!**	SonicOS Standard 3.0.0.0-16s	FRI NOV 12 14:55:26 2004	2.5 MB		
Uploaded Firmware with Factory Default Settings - **New!**	SonicOS Standard 3.0.0.0-16s	FRI NOV 12 14:55:26 2004	2.5 MB		
Uploaded Firmware with Backup Settings - **New!**	SonicOS Standard 3.0.0.0-16s	FRI NOV 12 14:55:26 2004	2.5 MB		

Settings

Import Settings

To import a previously saved preferences file into the SonicWALL security appliance, follow these instructions:

1. Click **Import Settings** to import a previously exported preferences file into the SonicWALL security appliance. The **Import Settings** window is displayed.
2. Click **Browse** to locate the file which has a *.exp file name extension.
3. Select the preferences file.
4. Click **Import**, and restart the firewall.

Export Settings

To export configuration settings from the SonicWALL security appliance, use the instructions below:

1. Click **Export Settings**.
2. Click **Export**.
3. Click **Save**, and then select a location to save the file. The file is named “sonicwall.exp” but can be renamed.
4. Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL security appliance if it is necessary to reset the firmware.

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Return your SonicWALL security appliance to the previous system state.

Note: *SonicWALL security appliance SafeMode, which uses the same settings used in the Firmware Management section, provides quick recovery from uncertain states.*

New Firmware

To receive automatic notification of new firmware, select the **Notify me when new firmware is available** check box. If you enable this feature, the SonicWALL security appliance sends a status message to the SonicWALL security appliance firmware server daily with the following information:

- **SonicWALL Serial Number**
- **Product Type**
- **Current Firmware Version**
- **Language**
- **Currently Available Memory**
- **ROM Version**
- **Options and Upgrades**

Alert: *After the initial 90 days from purchase, firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL security appliance at <https://www.mysonicwall.com>.*

Updating Firmware Manually

Click **Upload New Firmware** to load new firmware in the SonicWALL security appliance. A dialogue box is displayed warning you that your current firmware version is overwritten by the uploaded version. You should export your current SonicWALL security appliance settings to a preferences file before uploading new firmware. Click **Browse** to locate the new firmware version. Once you locate the file, click **Upload** to load the new firmware onto the SonicWALL security appliance.

Firmware Management Settings

The **Firmware Management** table has the following columns:

- **Firmware Image** - In this column, types of firmware images are listed:
    - **Current Firmware**, firmware currently loaded on the SonicWALL security appliance.
    - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
    - **Current Firmware with Backup Settings**, a firmware image created by clicking **Create Backup Settings**. This only displays after you create a backup image.
    - **Uploaded Firmware**, the last version uploaded from mysonicwall.com. This only displays after you upload new firmware.
    - **Uploaded Firmware with Factory Default Settings,** rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password. This only displays after you upload new firmware.
    - **Uploaded Firmware with Backup Settings**, a firmware image created by clicking **Create Backup Settings**. This only displays if you upload new firmware after you create a backup image.
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

Alert: *When uploading firmware to the SonicWALL security appliance, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.*

Note: *Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image. On the PRO 5060, the uploaded firmware images are removed from the table after rebooting the SonicWALL security appliance.*

SafeMode - Rebooting the SonicWALL Security Appliance

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. Pressing the Reset button for one second launches the SonicWALL security appliance into SafeMode. SafeMode allows you to select the firmware version to load and reboot the SonicWALL security appliance. To access the SonicWALL security appliance using SafeMode, press the Reset button for 1 second. After the SonicWALL security appliance reboots, open your Web browser and enter the current IP address of the SonicWALL security appliance or the default IP address: *192.168.168.168*. The SafeMode page is displayed:

SafeMode allows you to do any of the following:

- Upload and download firmware images to the SonicWALL security appliance.
- Upload and download system settings to the SonicWALL security appliance.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL security appliance to a previous system state.

System Information

System Information for the SonicWALL security appliance is retained and displayed in this section.

Firmware Management

The **Firmware Management** table has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:
    - **Current Firmware**, firmware currently loaded on the SonicWALL security appliance
    - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
    - **Current Firmware with Backup Settings**, a firmware image created by clicking **Create Backup Settings**. This only displays after you create a backup image.
    - **Uploaded Firmware**, the last version uploaded from mysonicwall.com
    - **Uploaded Firmware with Factory Default Settings,** rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
    - **Uploaded Firmware with Backup Settings**, a firmware image created by clicking **Create Backup Settings**. This only displays after you create a backup image.
- **Version** - The firmware version is listed in this column.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

Note: *Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.*

Click **Boot** in the firmware row of your choice to restart the SonicWALL security appliance.

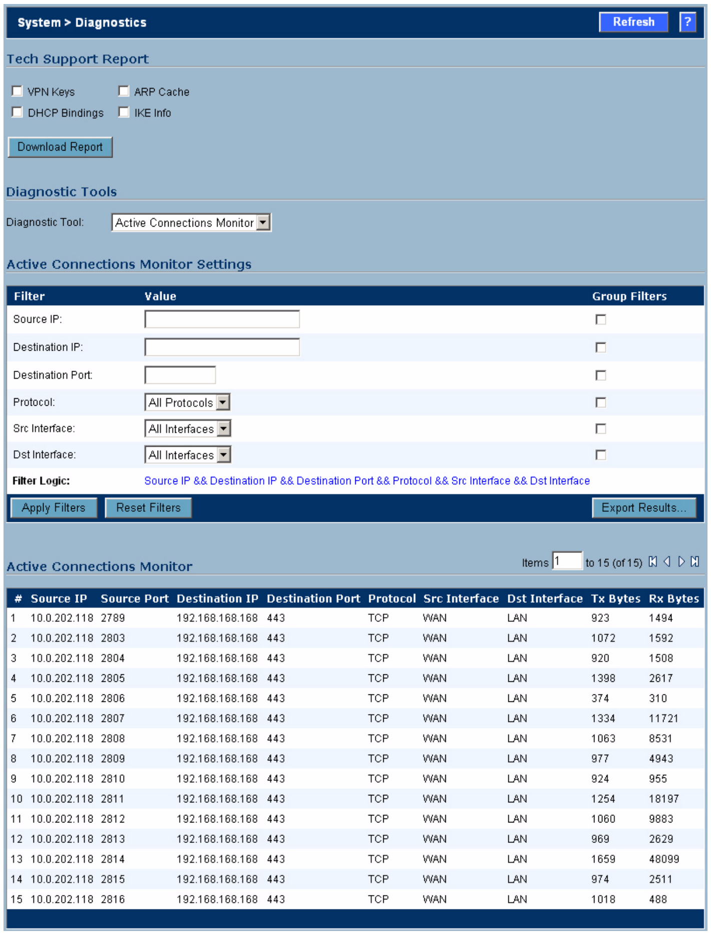
CHAPTER

8

Performing Diagnostic Tests and Restarting the SonicWALL Security Appliance

System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as CPU and Process Monitors.



Tech Support Report

☐ VPN Keys ☐ ARP Cache
☐ DHCP Bindings ☐ IKE Info

Diagnostic Tools

Diagnostic Tool: Active Connections Monitor

Active Connections Monitor Settings

Filter	Value	Group Filters
Source IP:		☐
Destination IP:		☐
Destination Port:		☐
Protocol:	All Protocols	☐
Src Interface:	All Interfaces	☐
Dst Interface:	All Interfaces	☐
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface	

Active Connections Monitor

Items 1 to 15 (of 15)

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.118	2789	192.168.168.168	443	TCP	WAN	LAN	923	1494
2	10.0.202.118	2803	192.168.168.168	443	TCP	WAN	LAN	1072	1592
3	10.0.202.118	2804	192.168.168.168	443	TCP	WAN	LAN	920	1508
4	10.0.202.118	2805	192.168.168.168	443	TCP	WAN	LAN	1398	2617
5	10.0.202.118	2806	192.168.168.168	443	TCP	WAN	LAN	374	310
6	10.0.202.118	2807	192.168.168.168	443	TCP	WAN	LAN	1334	11721
7	10.0.202.118	2808	192.168.168.168	443	TCP	WAN	LAN	1063	8531
8	10.0.202.118	2809	192.168.168.168	443	TCP	WAN	LAN	977	4943
9	10.0.202.118	2810	192.168.168.168	443	TCP	WAN	LAN	924	955
10	10.0.202.118	2811	192.168.168.168	443	TCP	WAN	LAN	1254	18197
11	10.0.202.118	2812	192.168.168.168	443	TCP	WAN	LAN	1060	9883
12	10.0.202.118	2813	192.168.168.168	443	TCP	WAN	LAN	969	2629
13	10.0.202.118	2814	192.168.168.168	443	TCP	WAN	LAN	1659	48099
14	10.0.202.118	2815	192.168.168.168	443	TCP	WAN	LAN	974	2511
15	10.0.202.118	2816	192.168.168.168	443	TCP	WAN	LAN	1018	488

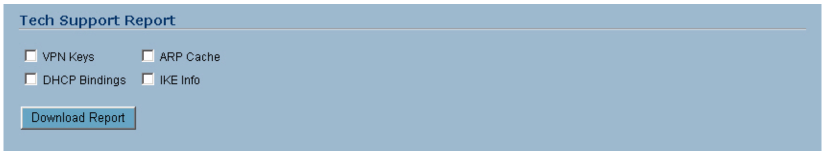
Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWALL security appliance configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.

▲ **Alert:** *You must register your SonicWALL security appliance on mySonicWALL.com to receive technical support.*

Before e-mailing the Tech Support Report to the SonicWALL Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWALL Technical Support to provide you with better service.

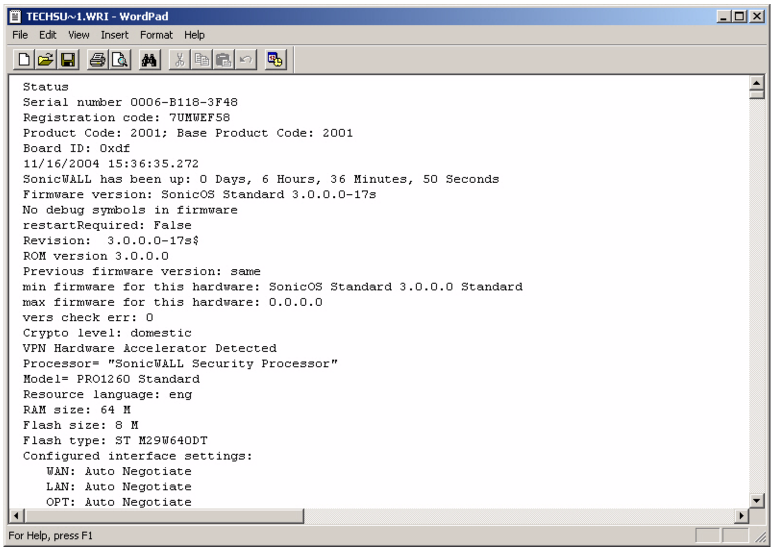
Generating a Tech Support Report



1. In the **Tech Support Report** section, select any of the following four report options:

- **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.
- **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.
- **DHCP Bindings** - saves entries from the SonicWALL security appliance DHCP server.
- **IKE Info** - saves current information about active IKE configurations.

2. Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.
3. Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.



```
Status
Serial number 0006-B118-3F48
Registration code: 7UMWEF58
Product Code: 2001; Base Product Code: 2001
Board ID: 0xdf
11/16/2004 15:36:35.272
SonicWALL has been up: 0 Days, 6 Hours, 36 Minutes, 50 Seconds
Firmware version: SonicOS Standard 3.0.0.0-17s
No debug symbols in firmware
restartRequired: False
Revision:  3.0.0.0-17s$
ROM version 3.0.0.0
Previous firmware version: same
min firmware for this hardware: SonicOS Standard 3.0.0.0 Standard
max firmware for this hardware: 0.0.0.0
vers check err: 0
Crypto level: domestic
VPN Hardware Accelerator Detected
Processor= "SonicWALL Security Processor"
Model= PRO1260 Standard
Resource language: eng
RAM size: 64 M
Flash size: 8 M
Flash type: ST M29W640DT
Configured interface settings:
   WAN: Auto Negotiate
   LAN: Auto Negotiate
   OPT: Auto Negotiate
```

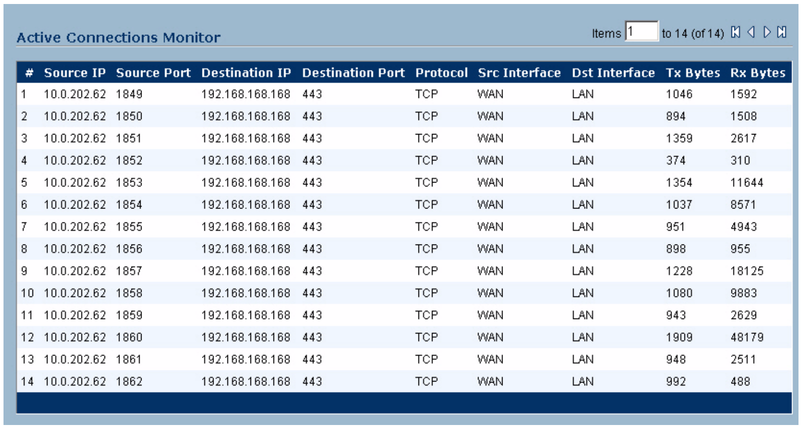
Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tools** menu in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- **Active Connections Monitor**
- **CPU Monitor**
- **DNS Name Lookup**
- **Find Network Path**
- **Packet Trace**
- **Ping**
- **Process Monitor**
- **Reverse Name Resolution**

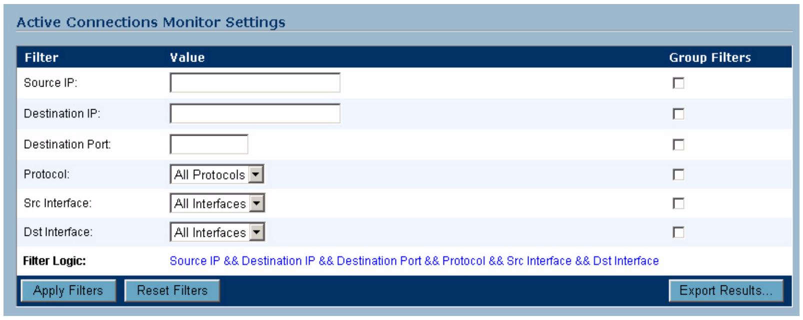
Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance.



#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.62	1849	192.168.168.168	443	TCP	WAN	LAN	1046	1592
2	10.0.202.62	1850	192.168.168.168	443	TCP	WAN	LAN	894	1508
3	10.0.202.62	1851	192.168.168.168	443	TCP	WAN	LAN	1359	2617
4	10.0.202.62	1852	192.168.168.168	443	TCP	WAN	LAN	374	310
5	10.0.202.62	1853	192.168.168.168	443	TCP	WAN	LAN	1354	11644
6	10.0.202.62	1854	192.168.168.168	443	TCP	WAN	LAN	1037	8571
7	10.0.202.62	1855	192.168.168.168	443	TCP	WAN	LAN	951	4943
8	10.0.202.62	1856	192.168.168.168	443	TCP	WAN	LAN	898	955
9	10.0.202.62	1857	192.168.168.168	443	TCP	WAN	LAN	1228	18125
10	10.0.202.62	1858	192.168.168.168	443	TCP	WAN	LAN	1080	9883
11	10.0.202.62	1859	192.168.168.168	443	TCP	WAN	LAN	943	2629
12	10.0.202.62	1860	192.168.168.168	443	TCP	WAN	LAN	1909	48179
13	10.0.202.62	1861	192.168.168.168	443	TCP	WAN	LAN	948	2511
14	10.0.202.62	1862	192.168.168.168	443	TCP	WAN	LAN	992	488

Active Connections Monitor Settings



Filter	Value	Group Filters
Source IP:		☐
Destination IP:		☐
Destination Port:		☐
Protocol:	All Protocols	☐
Src Interface:	All Interfaces	☐
Dst Interface:	All Interfaces	☐
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface	

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND.** For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

```
Source IP AND Destination IP
```

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

```
(Source IP OR Destination IP) AND Protocol
```

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

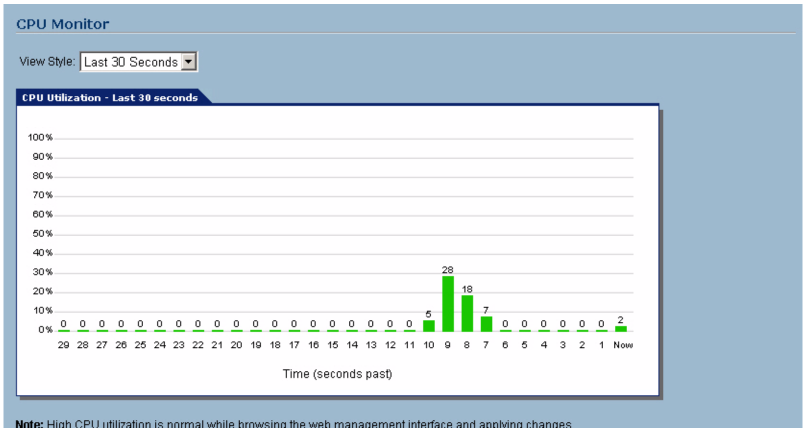
The connections are listed in the **Active Connections Monitor** table. The table lists:

- **Source IP**
- **Source Port**
- **Destination IP**
- **Destination Port**
- **Protocol**
- **Tx Bytes**
- **Rx Bytes**

Click on a column heading to sort by that column.

CPU Monitor

The **CPU Monitor** diagnostic tool shows real-time CPU utilization in second, minute, hour, and day intervals (historical data does not persist across reboots).



View Style: Last 30 Seconds

Note: High CPU utilization is normal while browsing the web management interface and applying changes

Note: *High CPU utilization is normal during Web-management page rendering, and while saving preferences to flash. Utilization by these tasks is an indication that available resources are being efficiently used rather than sitting idle. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and never experience starvation.*

DNS Name Lookup

The SonicWALL security appliance has a DNS lookup tool that returns the IP address of a domain name. Or, if you enter an IP address, it returns the domain name for that address.

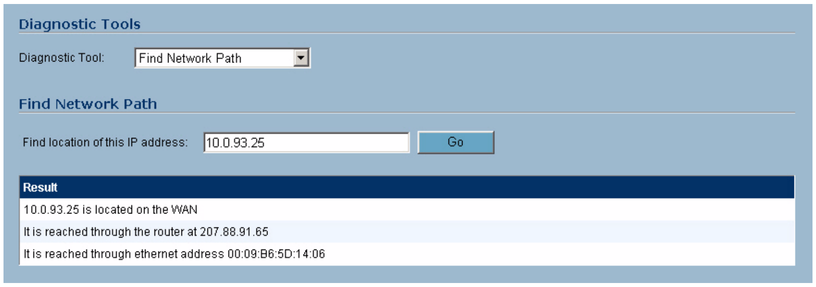
1. Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.

2 The SonicWALL security appliance queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWALL security appliance. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network > Settings** page.

Find Network Path

Find Network Path indicates if an IP host is located on the LAN or WAN ports. This can diagnose a network configuration problem on the SonicWALL security appliance. For example, if the SonicWALL security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.



Diagnostic Tool: Find Network Path

Find location of this IP address: 10.0.93.25

Result

10.0.93.25 is located on the WAN

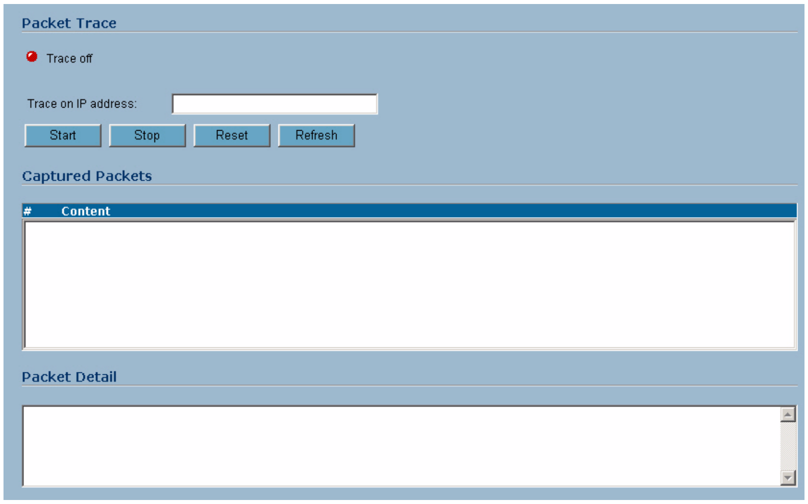
It is reached through the router at 207.88.91.65

It is reached through ethernet address 00:09:B6:5D:14:06

Find Network Path can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

Packet Trace

The **Packet Trace** tool tracks the status of a communications stream as it moves from source to destination. This is a useful tool to determine if a communications stream is being stopped at the SonicWALL security appliance, or is lost on the Internet.



To interpret this tool, it is necessary to understand the three-way handshake that occurs for every TCP connection. The following displays a typical three-way handshake initiated by a host on the SonicWALL security appliance LAN to a remote host on the WAN.

1 TCP received on LAN [SYN]

From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance receives SYN from LAN client.

2. TCP sent on WAN [SYN]
   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance forwards SYN from LAN client to remote host.

3. TCP received on WAN [SYN,ACK]
   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
   To 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

The SonicWALL security appliance receives SYN,ACK from remote host.

4. TCP sent on LAN [SYN,ACK]
   From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)
   To 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

The SonicWALL security appliance forwards SYN,ACK to LAN client.

5. TCP received on LAN [ACK]
   From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

Client sends a final ACK, and waits for start of data transfer.

6. TCP sent on WAN [ACK]
   From 207.88.211.116 / 1937 (00:40:10:0c:01:4e
   To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance forwards the client ACK to the remote host and waits for the data transfer to begin.

When using packet traces to isolate network connectivity problems, look for the location where the three-way handshake is breaking down. This helps to determine if the problem resides with the SonicWALL security appliance configuration, or if there is a problem on the Internet.

Select **Packet Trace** from the **Diagnostic tool** menu.

✓ **Tip:** *Packet Trace requires an IP address. The SonicWALL security appliance DNS Name Lookup tool can be used to find the IP address of a host.*

7. Enter the IP address of the remote host in the **Trace on IP address** field, and click **Start.** You must enter an IP address in the **Trace on IP address** field; do not enter a host name, such as “www.yahoo.com”. The **Trace is off** turns from red to green with Trace Active displayed.
8. Contact the remote host using an IP application such as Web, FTP, or Telnet.
9. Click **Refresh** and the packet trace information is displayed.
10. Click **Stop** to terminate the packet trace, and **Reset** to clear the results.

The **Captured Packets** table displays the packet number and the content of the packet, for instance, *ARP Request send on WAN 42 bytes*.

Select a packet in the **Captured Packets** table to display packet details. Packet details include the packet number, time, content, source of the IP address, and the IP address destination.

Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

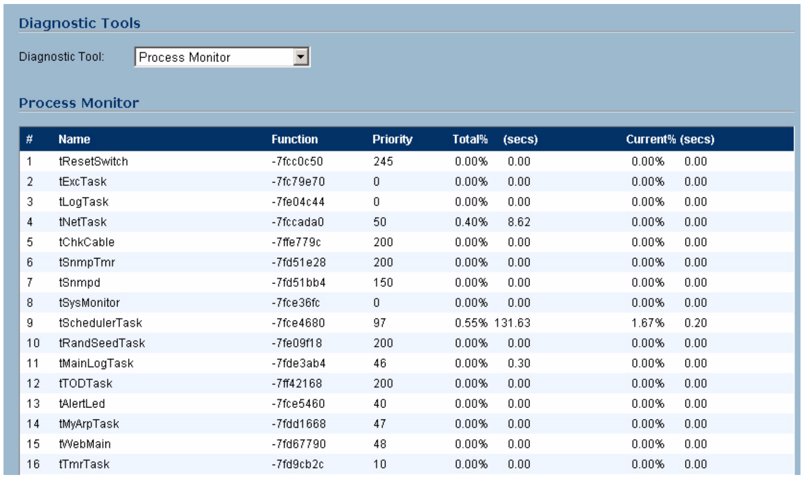
1 Select **Ping** from the **Diagnostic Tool** menu.

2 Enter the IP address or host name of the target device and click **Go**.

3 If the test is successful, the SonicWALL security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Process Monitor

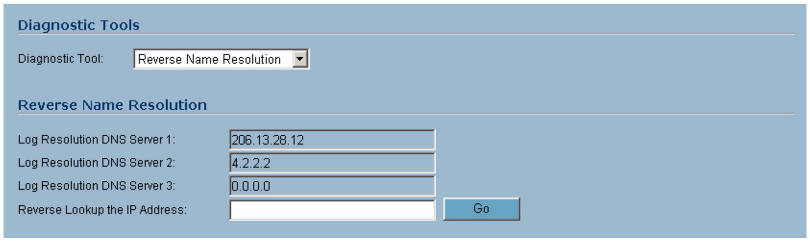
Process Monitor shows individual system processes, their CPU utilization, and their system time.



#	Name	Function	Priority	Total%	(secs)	Current% (secs)	
1	tResetSwitch	-7fcc0c50	245	0.00%	0.00	0.00%	0.00
2	tExcTask	-7fc79e70	0	0.00%	0.00	0.00%	0.00
3	tLogTask	-7fe04c44	0	0.00%	0.00	0.00%	0.00
4	tNetTask	-7fccada0	50	0.40%	8.62	0.00%	0.00
5	tChkCable	-7ffe779c	200	0.00%	0.00	0.00%	0.00
6	tSnmpTmr	-7fd51e28	200	0.00%	0.00	0.00%	0.00
7	tSnmpd	-7fd51bb4	150	0.00%	0.00	0.00%	0.00
8	tSysMonitor	-7fce36fc	0	0.00%	0.00	0.00%	0.00
9	tSchedulerTask	-7fce4680	97	0.55%	131.63	1.67%	0.20
10	tRandSeedTask	-7fe09f18	200	0.00%	0.00	0.00%	0.00
11	tMainLogTask	-7fde3ab4	46	0.00%	0.30	0.00%	0.00
12	tTODTask	-7ff42168	200	0.00%	0.00	0.00%	0.00
13	tAlertLed	-7fce5460	40	0.00%	0.00	0.00%	0.00
14	tMyArpTask	-7fdd1668	47	0.00%	0.00	0.00%	0.00
15	tWebMain	-7fd67790	48	0.00%	0.00	0.00%	0.00
16	tTmrTask	-7fd9cb2c	10	0.00%	0.00	0.00%	0.00

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.

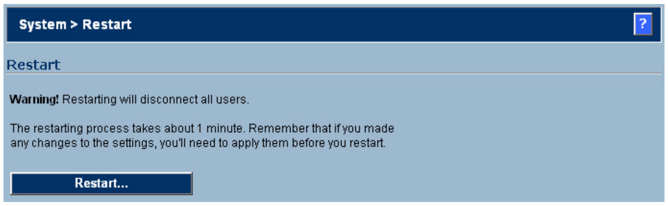


Log Resolution DNS Server 1: 206.13.28.12
Log Resolution DNS Server 2: 4.2.2.2
Log Resolution DNS Server 3: 0.0.0.0
Reverse Lookup the IP Address:

Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

System > Restart

Click **Restart** to display the **System > Restart** page.



Warning! Restarting will disconnect all users.

The restarting process takes about 1 minute. Remember that if you made any changes to the settings, you'll need to apply them before you restart.

The SonicWALL security appliance can be restarted from the Web Management interface. Click **Restart SonicWALL** and then click **Yes** to confirm the restart.

The SonicWALL security appliance takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

PART

3

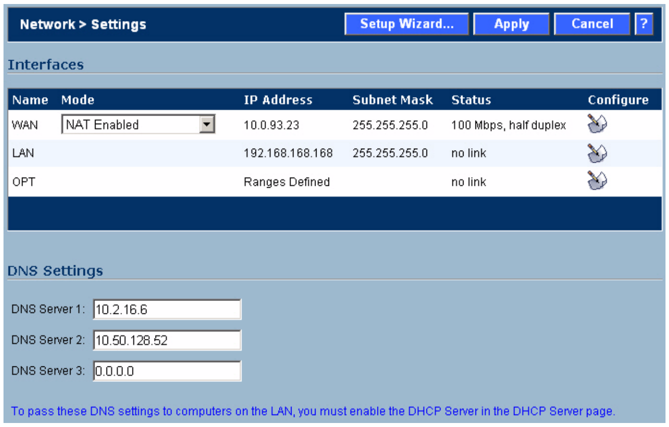
Network

CHAPTER 9

Configuring Network Settings

Network > Settings

The **Network > Settings** page allows you to configure the your network and Internet connectivity settings in the **Interface** table.



Interfaces

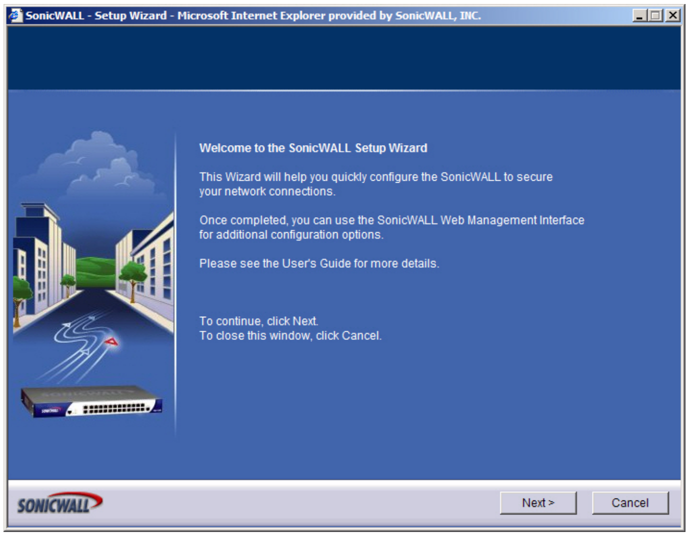
Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.23	255.255.255.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	no link	
OPT		Ranges Defined		no link	

DNS Settings

DNS Server 1: 10.2.16.6
DNS Server 2: 10.50.128.52
DNS Server 3: 0.0.0.0

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the DHCP Server page.

Setup Wizard


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

The **Setup Wizard** button accesses the **SonicWALL Setup Wizard**. offers a easy-to-use method for configuring your SonicWALL security appliance for the most common Internet connectivity options. If you are unsure about configuring network settings manually, use **SonicWALL Setup Wizard**.

Interfaces

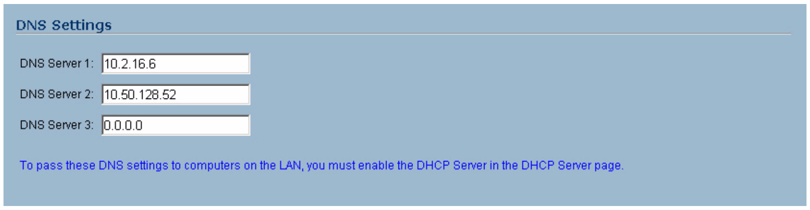
The **Interfaces** section displays the available network interfaces for your SonicWALL security appliance model. The Interfaces table lists the following information about the interfaces:

- **Name** - the name of the interface
- **Mode** - the network addressing mode (the WAN) interface
- **IP Address** - IP address assigned to the interface or whether ranges are defined for the Opt interface in Transparent mode.
- **Subnet Mask** - the network mask assigned to the subnet
- **Status** - the link status and speed
- **Configure** - click the edit icon to display the properties window for configuring the interface.

Interface Options by SonicWALL Security Appliance

SonicWALL Security Appliance Model	Interfaces
SonicWALL TZ 50	**WAN**, **LAN**
SonicWALL TZ 50 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL TZ 150	**WAN**, **LAN**
SonicWALL TZ 150 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL TZ 170	**WAN**, **LAN**, **OPT**
SonicWALL TZ 170 SP	**WAN**, **LAN**, **Modem**
SonicWALL TZ 170 Wireless	**WAN**, **LAN**, **WLAN**
SonicWALL PRO 1260	**WAN**, **LAN**, **OPT**
SonicWALL PRO 2040	**WAN, LAN, DMZ**
SonicWALL PRO 3060	**WAN**, **LAN**, **DMZ**

DNS Settings



DNS Server 1: 10.2.16.6

DNS Server 2: 10.50.128.52

DNS Server 3: 0.0.0.0

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the DHCP Server page.

DNS (Domain Name System) is a hierarchical system for identifying hosts on the Internet or on a private, corporate TCP/IP internetwork. It is a method for identifying hosts with friendly names instead of IP addresses as well as a method for locating hosts. Hosts are located by resolving their names into their associated IP addresses so network communication can be initiated with the host computer.

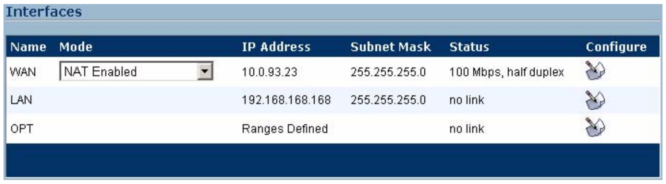
The DNS Settings setting information is automatically entered when you configure your WAN interface settings. Although, you can enter up to three IP addresses in the **DNS Settings** section if your WAN Internet connection using static IP addressing. However, at least one IP address of a DNS Server is required to resolve host names to IP addresses or IP addresses to host names.

Note: *It is strongly recommended to have at least two DNS IP addresses configured on the SonicWALL security appliance. This provides redundancy in the event one DNS server is unavailable.*

1. Enter the IP address in the **DNS Server 1** field.
2. Enter the second IP address in the **DNS Server 2** field.
3. Click **Apply** for the changes to take effect on the SonicWALL security appliance.

To pass DNS settings to computers on the LAN, you must enable the SonicWALL security appliance DHCP server on the **Network > DHCP** Server page.

Configuring the WAN Interface



Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.23	255.255.255.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	no link	
OPT		Ranges Defined		no link	

The **Mode** menu in the **Interfaces** table for the WAN interface determines the network address scheme of your SonicWALL security appliance. It includes six options:

- **Transparent Mode** enables the SonicWALL security appliance to bridge the WAN subnet onto the LAN interface. It requires valid IP addresses for all computers on your network, but allows remote access to authenticated users. Your public WAN IP address is visible to the Internet.
- **NAT Enabled** mode translates the private IP addresses on the network to the single, valid IP address of the SonicWALL security appliance. Select **NAT Enabled** if your ISP assigned you only one or two valid IP addresses.
- **NAT with DHCP Client** mode configures the SonicWALL security appliance to request IP settings from a DHCP server on the Internet. **NAT with DHCP Client** is a typical network addressing mode for cable and DSL customers.
- **NAT with PPPoE** mode uses PPPoE to connect to the Internet. If desktop software and a user name and password is required by your ISP, select **NAT with PPPoE**.
- **NAT with L2TP Client** mode uses IPSec to connect a L2TP server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.
- **NAT with PPTP Client** mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.

Configuring Transparent Mode

Transparent Mode requires valid IP addresses for all computers on your network, and allows remote access to authenticated users. Your public WAN IP address is visible to the Internet. To enable Transparent Mode, select **Transparent Mode** from the **Mode** menu. The WAN and LAN IP addresses are now identical. To complete the configuration, click **Intranet** in the **Network** menu list.

1. Select **Specified address ranges are attached to the LAN link**.
2. Click **Add** in the **From Address** table.
3. Enter the range of network IP addresses on the LAN.
4. Click **OK** and then click **Apply**.
5. Click **Restart** in the Status bar of the management interface. The SonicWALL security appliance restarts and updates the configuration.

Configuration Example

Your ISP has given you a public IP address of 66.217.71.191 and a range of public IP address from 66.217.71.192 to 66.217.71.200. To configure the SonicWALL security appliance in Transparent Mode, select **Transparent Mode** from the **Mode** menu. Then follow these steps:

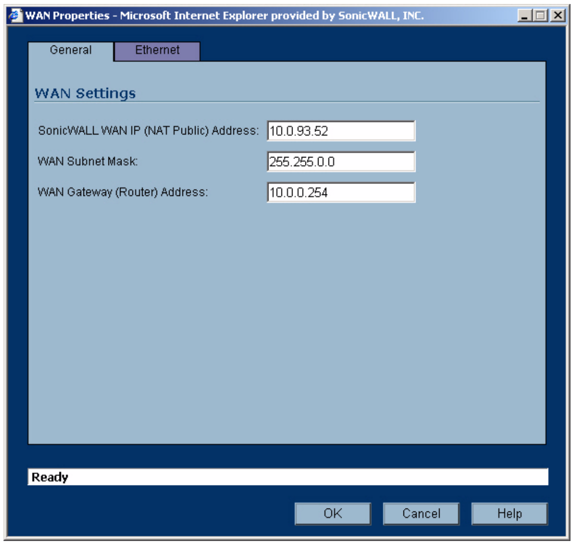
1. Click the icon in the **Configure** column to display the **WAN Settings** window.
2. Enter your IP address, 66.217.71.191, in the **WAN IP Address** field. Complete the rest of the fields in the **WAN Settings** window using information provided by the ISP.
3. Click **OK**.
4. Click **Intranet** in the **Network** menu list.
5. Select **Specified address ranges are attached to the LAN link**.
6. Click **Add** in the **LAN/WAN Client Address Ranges** table.
7. Enter your IP address, 66.217.71.192, in the **IP Address From** field.
8. Enter the IP address, 66.217.71.200, in the **IP Address To** field and click **OK.**
9. Click **Apply**, and then **Restart** in the **Status** bar. The SonicWALL security appliance restarts and updates the configuration.

Configuring NAT Enabled

If your ISP provides a static IP address for your Internet connection, use the **NAT Enabled**.

1 Select **NAT Enabled** from the drop-down menu in the **Mode** column of the **Interfaces** table.

2 Click on the edit icon in the **Configure** column of the **WAN** interface. The **WAN Properties** window is displayed.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Settings

SonicWALL WAN IP (NAT Public) Address: 10.0.93.52

WAN Subnet Mask: 255.255.0.0

WAN Gateway (Router) Address: 10.0.0.254

Ready

3 In the **WAN Settings** section, enter a valid public IP address in the **SonicWALL WAN IP (NAT Public) Address** field.

4 Enter the subnet mask in the **WAN Subnet Mask** field.

5 Enter the IP address of the router in the **WAN Gateway (Router) Address** field.

6 Click **OK**.

Configuring NAT with DHCP Client

If your ISP did not provide you with a public IP address, the SonicWALL security appliance can obtain an IP address from a DHCP server at the ISP. NAT with DHCP Client is typically used with cable and DSL connections. To configure NAT with DHCP Client, log into the SonicWALL security appliance and click **Network**.

1 Select **NAT with DHCP Client** from the drop-down menu in the **Mode** column of the **Interfaces** table.

2 Click the edit icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.

3 Enter the host name assigned to you by your ISP in the **Host Name** field. (Optional)

4 Click **Renew** to obtain new IP address settings for the SonicWALL security appliance.

5 Click **Release** to remove the IP address settings from the SonicWALL security appliance. Click **Refresh** to reload the current settings into the SonicWALL security appliance.

6 Click **OK**.

Note: *DNS Settings are obtained automatically when the SonicWALL security appliance receives its IP address information from the DHCP Server.*

Configuring NAT with PPPoE Client

The SonicWALL security appliance can use Point-to-Point Protocol over Ethernet to connect to the Internet. If your ISP requires the installation of desktop software as well as a user name and password to access the Internet, enable NAT with PPPoE Client.

1. Select **NAT with PPPoE Client** from the drop-down menu in the **Mode** column of the **Interfaces** table.
2. Click the edit icon in the WAN entry of the **Interfaces** table. The **WAN Properties** window is displayed.
3. Select **Obtain an IP Address Automatically** if you do not have a public IP address from your ISP. If you have an IP address from your ISP, select **Use the following Address**, and enter the IP address in the IP address field.
4. Click the **PPPoE** tab.
5. Enter your user name and password provided by your ISP in the **User Name** and **User Password** fields.
6. Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity. 10 minutes is the default value.
7. Click **OK**.

Configuring NAT with L2TP Client

If your Internet connection is provided through a L2TP server, you must configure the SonicWALL security appliance to use NAT with L2TP Client. L2TP (Layer 2 Tunneling Protocol) provides interoperability between VPN vendors that protocols such as Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F) do not have.

1. Log into the SonicWALL security appliance, and click **Network**.
2. Select **NAT with L2TP Client** from the **Network Addressing Mode** menu.
3. Click the edit icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.
4. **Obtain an IP Address Automatically** is selected by default. Enter your host name in the **Host Name** field. Click **Renew** to obtain new IP addressing information. Click **Release** to discard IP addressing information. Click **Refresh** to reload the IP addressing information.
5. If you have IP addressing information, select **Use the following IP Address**.
6. Enter your public IP address in the **SonicWALL WAN IP (NAT Public) Address** field.
7. Enter the WAN Subnet information in the **WAN Subnet Mask** field.
8. Enter the WAN Gateway IP address in the **WAN Gateway (Router) Address** field.
9. Click on the **L2TP** tab.
10. Enter your user name in the **User Name** field.
11. Enter your password in the **User Password** field.
12. Enter the IP address of the L2TP Server in the **L2TP Server IP Address** field.
13. Enter the host name of the L2TP Server in the **L2TP Host Name** field.
14. Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity.
15. Once a connection is established, the SonicWALL security appliance WAN IP address, the Gateway address and the DNS Server IP addresses are displayed in the **Settings Acquired via L2TP** section.
16. Click **OK**.

Configuring NAT with PPTP Client

If your Internet connection is provided through a PPTP server, you must configure the SonicWALL security appliance to use NAT with PPTP Client.

Log into the SonicWALL security appliance, and click **Network**.

1 Select **NAT with PPTP Client** from the **Network Addressing Mode** menu.

2 Click the edit icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.

3 **Obtain an IP Address Automatically** is selected by default. Enter your host name in the **Host Name** field. Click **Renew** to obtain new IP addressing information. Click **Release** to discard IP addressing information. Click **Refresh** to reload the IP addressing information.

4 If you have IP addressing information, select **Use the following IP Address**.

5 Enter the WAN IP address in the **SonicWALL WAN IP (NAT Public) Address** field.

6 Enter the WAN Subnet information in the **WAN Subnet Mask** field.

7 Enter the WAN Gateway IP address in the **WAN Gateway (Router) Address** field.

8 Click on the **PPTP** tab.

9 Enter your user name in the **User Name** field.

10 Enter your password in the **User Password** field.

11 Enter the IP address of the PPTP Server in the **PPTP Server IP Address** field.

12 Enter the host name of the PPTP Client in the **PPTP (Client) Host Name** field.

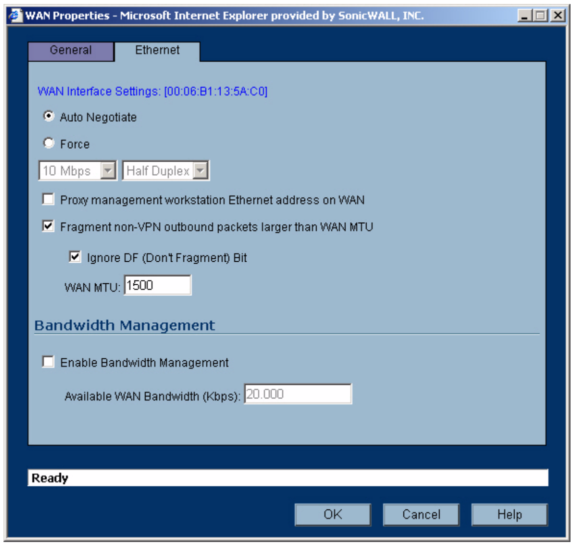
13 Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity.

14 Once a connection is established, the SonicWALL security appliance WAN IP address, the Gateway address and the DNS Server IP addresses are displayed in the **Settings Acquired via PPTP** section.

15 Click **OK**.

Configuring Ethernet Settings in WAN Properties

The **Ethernet** tab in the **WAN Properties** window allows you to manage the Ethernet settings of the WAN interface. For most networks, you do not need to make any changes on this page.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
Bandwidth Management
OK
Cancel
Help

WAN Interface Settings: [00:06:B1:13:5A:C0]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

☐ Proxy management workstation Ethernet address on WAN

☑ Fragment non-VPN outbound packets larger than WAN MTU

☑ Ignore DF (Don't Fragment) Bit

WAN MTU: 1500

☐ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

Ready

The **WAN Interface Settings** information at the top of the **Ethernet** page is the Ethernet address of the WAN interface on the SonicWALL security appliance.

Auto Negotiate is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

If you select **Force**, an information dialog is displayed with the following message:

Note: *Disabling Auto Negotiate on this interface will also disable AutoMDIX on this interface. You may need to switch from a straight-through Ethernet cable to a cross over Ethernet cable, or vice-versa. Click OK to proceed.*

Select **Proxy management workstation Ethernet address on WAN** if you are managing the Ethernet connection from the LAN side of your network. The SonicWALL security appliance takes the Ethernet address of the computer managing the SonicWALL security appliance and proxies that address onto the WAN port of the SonicWALL security appliance. For instance, if your ISP is using the MAC address of your network card for identification, you can proxy the MAC address of your network card onto the SonicWALL WAN port.

✓ **Tip:** *If you are not managing the Ethernet connection from the LAN, the SonicWALL security appliance looks for a random computer on the network creating a lengthy search process.*

Note: *If you enable this feature, it may take the SonicWALL a lengthy period of time to locate the management station.*

Fragment non-VPN outbound packets larger than WAN MTU is selected by default with a default **WAN MTU** value of 1500 based on the Ethernet standard MTU. Specifies all non-VPN outbound packets larger than this Interface’s MTU be fragmented. The minimum value is 68. Decreasing the packet size can improve network performance as large packets require more network transmissions when a router cannot handle the packet size. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.

Ignore Don’t Fragment (DF) Bit - Overrides DF bits in packets.

Select **Enable Bandwidth Management** to allocate bandwidth resources to critical applications on the your network. Enter the total bandwidth available in the **Available WAN Bandwidth (Kbps)** field.

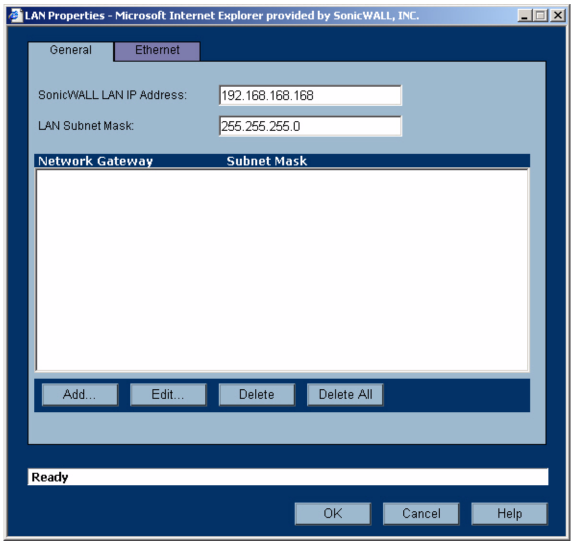
20.00 Kbps is the default available WAN bandwidth.

▲ **Alert:** *Bandwidth management is only available on outbound network traffic.*

Configuring the LAN Interface

Basic LAN Configuration

1 Click on the edit icon in the **Configure** column of the **LAN** information. The **LAN Properties** window is displayed.



LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

SonicWALL LAN IP Address: 192.168.168.168

LAN Subnet Mask: 255.255.255.0

Ready

2 In the **General Settings** section, enter a valid private IP address in the **SonicWALL LAN IP** field.

3 Enter the subnet mask in the **LAN Subnet Mask** field.

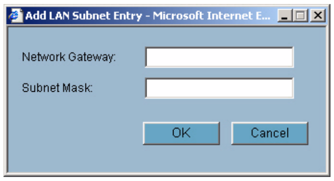
4 Click **OK**.

Configuring Multiple LAN Subnets

This multiple LAN subnet feature supports legacy networks incorporating the SonicWALL security appliance, as well as enable you to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL security appliance. All users on the subnet must use this address as their default router/gateway address.

1 Click on the edit icon in the **Configure** column of the **LAN** information. The **LAN Properties** window is displayed.

2 Click **Add**. The **Add LAN Subnet Entry** window is displayed.



Add LAN Subnet Entry - Microsoft Internet E...

3 Enter the additional LAN IP address in the **IP Address** field.

4 Enter the subnet in the **Subnet Mask** field. You can edit or delete any LAN subnet entries.

Select an entry and click **Edit** to change the information.

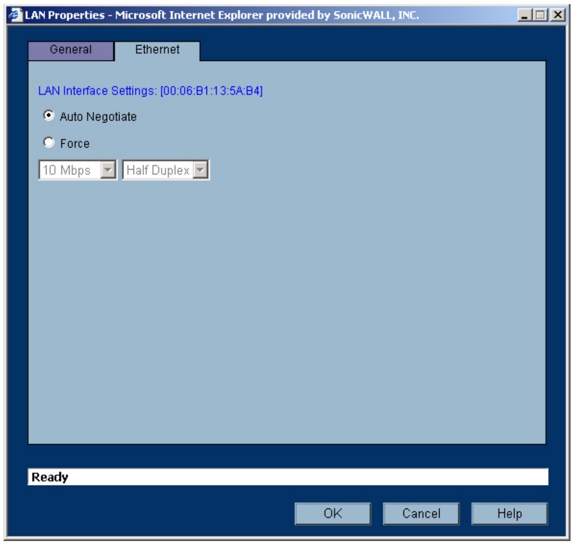
Select an entry and click **Delete** to remove the entry from the table.

Click **Delete All** to remove all the entries in the table.

5 Click **OK**.

Configuring Ethernet Settings

The **Ethernet** tab in the **LAN Properties** window allows you to manage the Ethernet settings of LAN interface. For most networks, you do not need to make any changes on this page.


LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
OK
Cancel
Help

LAN Interface Settings: [00:06:B1:13:5A:B4]

● Auto Negotiate

○ Force

10 Mbps

Half Duplex

Ready

The **LAN Interface Settings** information at the top of the **Ethernet** page is the Ethernet address of the LAN interface on the SonicWALL security appliance.

Auto Negotiate is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

If you select **Force**, an information dialog is displayed with the following message:

Note: *Disabling Auto Negotiate on this interface will also disable AutoMDIX on this interface. You may need to switch from a straight-through Ethernet cable to a cross over Ethernet cable, or vice-versa. Click OK to proceed.*

Configuring the OPT Interface

You can configure the OPT interface in either Transparent Mode or NAT Mode:

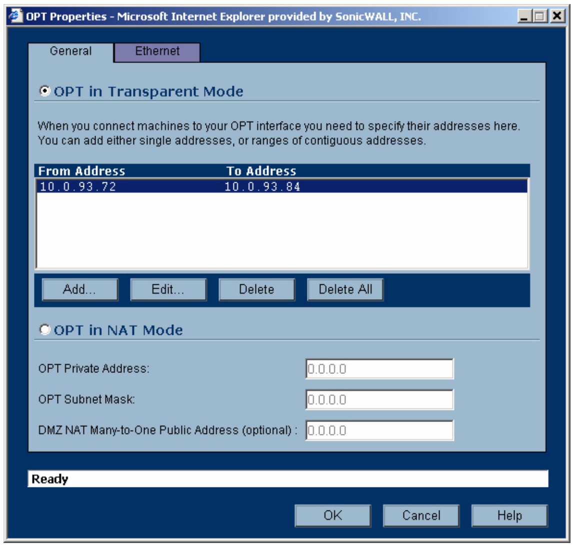
- **Transparent Mode** enables the SonicWALL security appliance to bridge the OPT subnet onto the WAN interface. It requires valid IP addresses for all computers connected to the OPT interface on your network, but allows remote access to authenticated users. You can use the OPT interface in Transparent mode for public servers and devices with static IP addresses you want visible outside your SonicWALL security appliance-protected network.
- **NAT** Mode translates the private IP addresses of devices connected to the OPT interface to a single, static IP address.

Configuring Transparent Mode

Transparent Mode requires valid IP addresses for all computers on your network, and allows remote access to authenticated users.

To enable Transparent Mode:

1. Click the Edit Icon in the line for the OPT interface in the Interfaces table. The OPT Properties window displays.


OPT Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

● OPT in Transparent Mode

When you connect machines to your OPT interface you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

From Address	To Address
10.0.93.72	10.0.93.84

○ OPT in NAT Mode

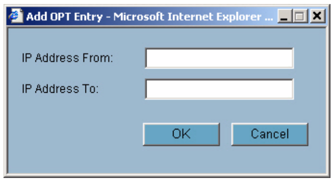
OPT Private Address: 0.0.0.0

OPT Subnet Mask: 0.0.0.0

DMZ NAT Many-to-One Public Address (optional) : 0.0.0.0

Ready

2. Select **OPT in Transparent Mode**. The OPT and WAN IP addresses are now identical.
3. To add an address or range of addresses, click **Add** below the address range list. The **Add Opt Entry** dialog box displays.


Add OPT Entry - Microsoft Internet Explorer ...
IP Address From:
IP Address To:
OK
Cancel

4. Enter a single IP address or the beginning of a range of IP addresses in the **IP Address From** field.

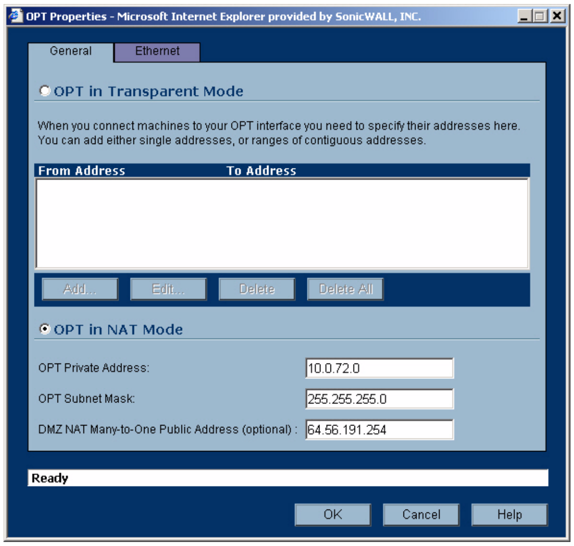
Note: *The address or range of addresses must be within the available range of IP addresses for your WAN interface.*

5. For a range of IP addresses, enter the ending address in the **IP Address To** field.
6. Click **OK** and then click **Apply**.

Configuring NAT Mode

NAT Enabled mode gives the OPT interface a single IP address and a subnet of available IP address. The IP addresses of devices connecting to the OPT interface are translated to the single OPT interface IP address.

1. Click the Edit Icon in the line for the OPT interface in the Interfaces table. The OPT Properties window displays.



○ OPT in Transparent Mode

When you connect machines to your OPT interface you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

● OPT in NAT Mode

OPT Private Address: 10.0.72.0

OPT Subnet Mask: 255.255.255.0

DMZ NAT Many-to-One Public Address (optional) : 64.56.191.254

Ready

2. Select **OPT in NAT Mode**.
3. Enter an IP address in the **OPT Private Address** field.
4. Enter the subnet mask in the **OPT Subnet Mask** field.
5. If you want to use the OPT interface as a DMZ, enter a publicly visible IP address in the **DMZ NAT Many-to-One Public Address** field. This address will be visible to the internet for public servers in your network.
6. Click **OK**.

Configuring the DMZ Interface

You can configure the DMZ interface in either Transparent Mode or NAT Mode:

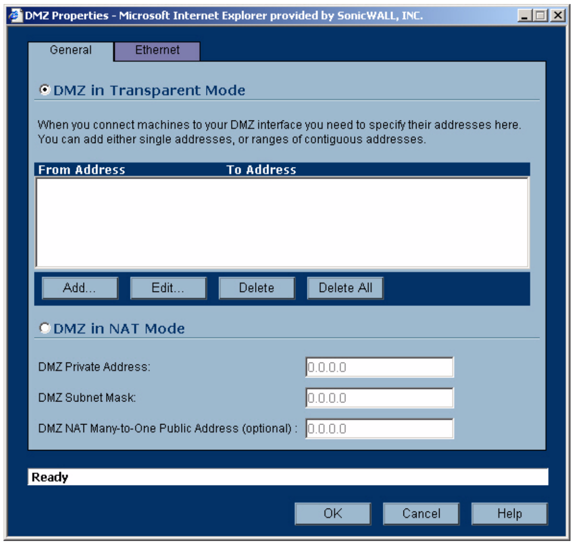
- **Transparent Mode** enables the SonicWALL security appliance to bridge the DMZ subnet onto the WAN interface. It requires valid IP addresses for all computers connected to the DMZ interface on your network, but allows remote access to authenticated users. You can use the DMZ interface in Transparent mode for public servers and devices with static IP addresses you want visible outside your SonicWALL security appliance-protected network.
- **NAT** Mode translates the private IP addresses of devices connected to the DMZ interface to a single, static IP address.

Configuring Transparent Mode

Transparent Mode requires valid IP addresses for all computers on your network, and allows remote access to authenticated users.

To enable Transparent Mode:

1 Click the Edit Icon in the line for the DMZ interface in the Interfaces table. The **DMZ Properties** window displays.


DMZ Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
From Address
To Address
Add...
Edit...
Delete
Delete All
Ready
OK
Cancel
Help

● DMZ in Transparent Mode

When you connect machines to your DMZ interface you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

○ DMZ in NAT Mode

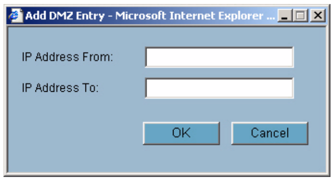
DMZ Private Address: 0.0.0.0

DMZ Subnet Mask: 0.0.0.0

DMZ NAT Many-to-One Public Address (optional) : 0.0.0.0

2 Select **DMZ in Transparent Mode**. The OPT and WAN IP addresses are now identical.

3 To add an address or range of addresses, click **Add** below the address range list. The **Add DMZ Entry** dialog box displays.


Add DMZ Entry - Microsoft Internet Explorer ...
IP Address From:
IP Address To:
OK
Cancel

4 Enter a single IP address or the beginning of a range of IP addresses in the **IP Address From** field.

Note: *The address or range of addresses must be within the available range of IP addresses for your WAN interface.*

5 For a range of IP addresses, enter the ending address in the **IP Address To** field.

6 Click **OK** and then click **Apply**.

Configuring NAT Mode

NAT Mode gives the DMZ interface a single IP address and a subnet of available IP address. The IP addresses of devices connecting to the DMZ interface are translated to the single DMZ interface IP address.

1 Click the edit icon in the line for the DMZ interface in the **Interfaces** table. The **DMZ Properties** window displays.

2 Select **DMZ in NAT Mode**.

3 Enter an IP address in the **DMZ Private Address** field.

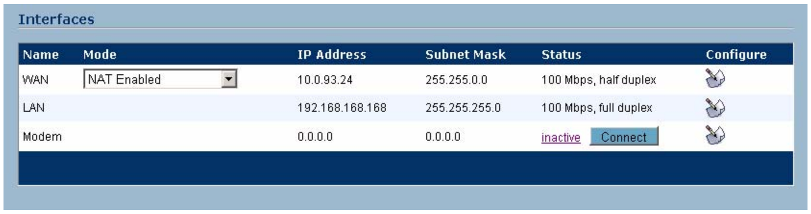
4 Enter the subnet mask in the **DMZ Subnet Mask** field.

5 To use the DMZ interface as a DMZ, enter a publicly visible IP address in the **DMZ NAT Many-to-One Public Address** field. This address will be visible to the Internet for public servers in your network.

6 Click **OK**.

Configuring the Modem Interface (TZ 170 SP)

The SonicWALL TZ 170 SP includes the **Modem** interface in the **Interfaces** table on the **Network > Settings** page.

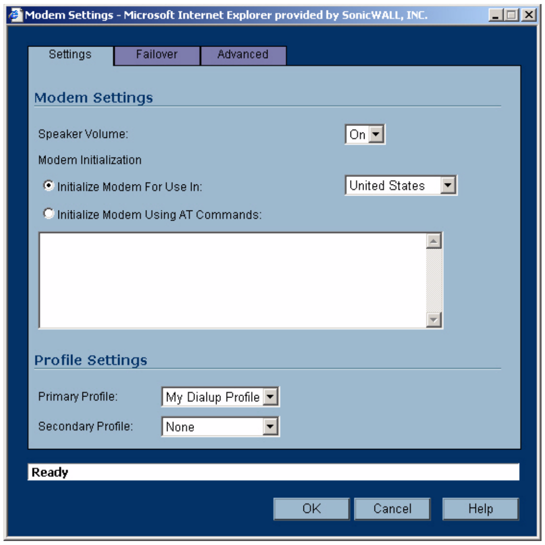


Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.24	255.255.0.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	100 Mbps, full duplex	
Modem		0.0.0.0	0.0.0.0	inactive Connect	

Clicking the edit icon for the **Modem** interface displays the **Modem Settings** window for configuring the modem properties.

Settings


Modem Settings - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Failover
Advanced
OK
Cancel
Help

Modem Settings

Speaker Volume: On

Modem Initialization

● Initialize Modem For Use In: United States

○ Initialize Modem Using AT Commands:

Profile Settings

Primary Profile: My Dialup Profile

Secondary Profile: None

Ready

Modem Settings

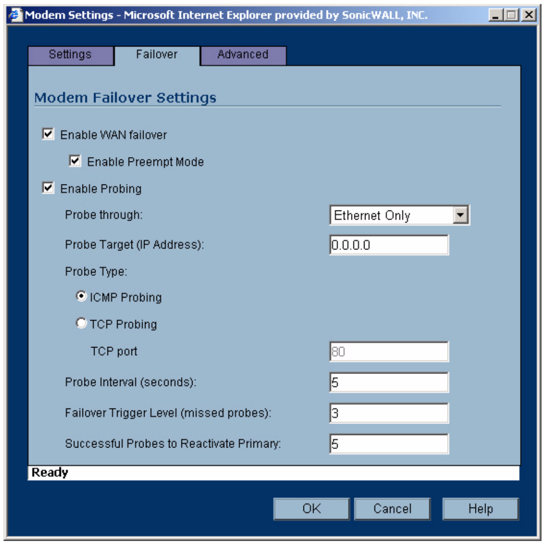
Speaker Volume - choose **On** or **Off** for your modem speaker volume. The default is **On**.

Modem Initialization - You can specify the country to initialize your modem by choosing **Initialize Modem For Use In** and specifying the country from the menu or specify the initialization of your modem using AT commands by selecting **Initialize Modem Using AT Commands** and entering your AT Commands in the text field.

Profiles

Select your primary profile from the **Primary Profile** menu. You create the profiles for this menu in the **Modem > Dialup Profiles** page. If you have more than one dial-up ISP account, you can specify a secondary profile from the **Secondary Profile** menu.

Failover


Modem Settings - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Failover
Advanced
Ready
OK
Cancel
Help

Modem Failover Settings

☑ Enable WAN failover

☑ Enable Preempt Mode

☑ Enable Probing

Probe through: Ethernet Only

Probe Target (IP Address): 0.0.0.0

Probe Type:

● ICMP Probing

○ TCP Probing

TCP port: 80

Probe Interval (seconds): 5

Failover Trigger Level (missed probes): 3

Successful Probes to Reactivate Primary: 5

The **Failover** page in the **Modem Setting** window includes the same settings on the **Modem > Failover** page. If you configured the failover settings on the **Modem > Failover** page, they are displayed in the **Failover** page. If you have not configured Failover settings, use the following instructions to configure the **Failover Settings**:

1. Select **Enable WAN Failover**.
2. Select **Enable Preempt Mode** if you want the primary WAN Ethernet interface to take over from the secondary modem WAN interface when it becomes active after a failure. If you do not enable **Pre-empt Mode**, the secondary WAN modem interface remains active as the WAN interface until you click **Disconnect**.
3. Select **Enable Probing**. Probing for WAN connectivity occurs over the Ethernet connection, the dial-up connection, or both. When probing is disabled on the Ethernet link, the SonicWALL security appliance only performs link detection. If the Ethernet connection is lost for a duration of 5-9 seconds, the SonicWALL security appliance considers the Ethernet connection to be unavailable. If the Ethernet link is lost for 0-4 seconds, the SonicWALL security appliance does not consider the connection to be lost. If you are swapping cables quickly, unnecessary WAN failover does not occur on the SonicWALL security appliance. If probing is enabled and the cable is unplugged, the 5-9 seconds link detection does not occur. Instead, the probing rules apply to the connection using the parameters configured for **Probe Interval (seconds)** and **Failover Trigger Level (missed probes)** settings. If probing is enabled on dialup, the dialup connection is terminated and re-established when probing fails over the modem.
4. Select an option from the **Probe through** menu. Select **Ethernet Only** to probe the Ethernet WAN connection and failover to the modem when the connection is lost. Select **Modem Only** to probe a dial-up connection and have the modem redial when the dial-up connection is lost. Select **Modem and Ethernet** to enable both types of probing on the SP.
5. Enter the IP address for the probe target in the **Probe Target (IP Address)** field. The Probe IP address is a static IP address on the WAN. If this field is left blank, or 0.0.0.0 is entered as the address, the Probe Target is the WAN Gateway IP address.

Note: *The probe is a **ping** sent to the specified IP address to determine Internet connectivity.*

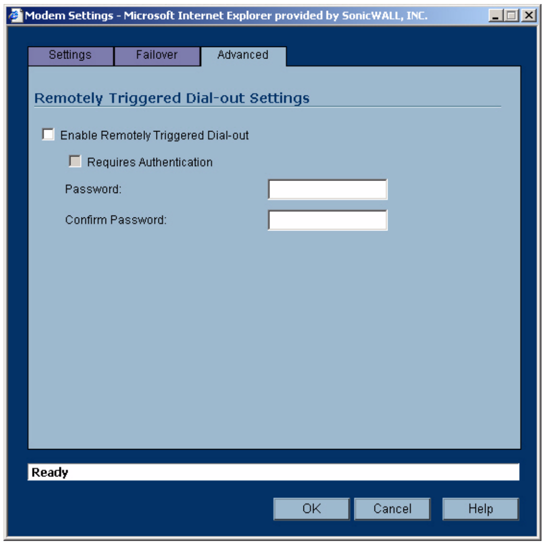
6. Select **ICMP Probing** or **TCP Probing** from the **Probe Type** options. If you select **TCP Probing**, enter the TCP port number in the **TCP port** field.
7. In the **Probe Interval (seconds)** field, enter the amount of time between probes to the **Probe Target**. The default value is **5** seconds. To deactivate the Probe Detection feature, enter *0* as the

value. In this case, the WAN failover only occurs when loss of the physical WAN Ethernet connection occurs on the SonicWALL security appliance.

8 Enter the number of missed probes required for the WAN failover to occur in the **Failover Trigger Level (missed probes)** field.

9 Enter a value for the number of successful probes required to reactivate the primary connection in the **Successful Probes to Reactivate Primary** field. The default value is five (5). By requiring a number of successful probes before the SonicWALL security appliance returns to its primary connection, you can prevent the SonicWALL security appliance from returning to the primary connection before the primary connection becomes stable.

Advanced


Modem Settings - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Failover
Advanced
OK
Cancel
Help

Remotely Triggered Dial-out Settings

☐ Enable Remotely Triggered Dial-out

☐ Requires Authentication

Password:

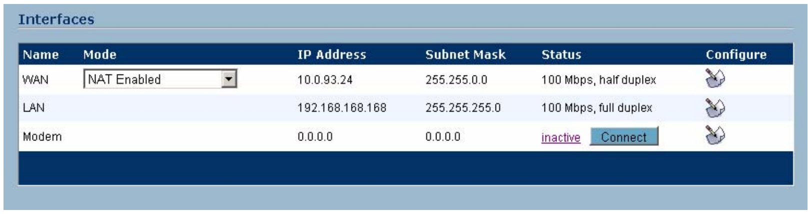
Confirm Password:

Ready

The **Advanced** page allows you remotely trigger the modem to dial-out to establish an WAN connection. Selecting **Enable Remotely Triggered Dial-out** configures the modem to accept remotely triggered dial-out.

If you check **Requires Authentication**, enter a password in the **Password** and **Confirm Password** fields. You will be prompted for a password before being allowed to trigger a dial-out.

Activating the Modem



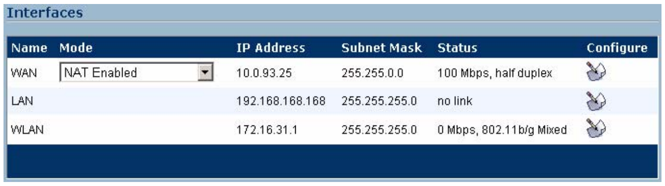
Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.24	255.255.0.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	100 Mbps, full duplex	
Modem		0.0.0.0	0.0.0.0	inactive Connect	

If the modem is inactive, an **inactive** link and **Connect** button are displayed in the **Status** column of the **Interfaces** table on the **Network>Settings** page. Clicking the Connect button establishes your modem connection. Once the connection is established, the **inactive** link and **Connect** button change to **active** and **Disconnect**.

Configuring WLAN Properties (TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless)

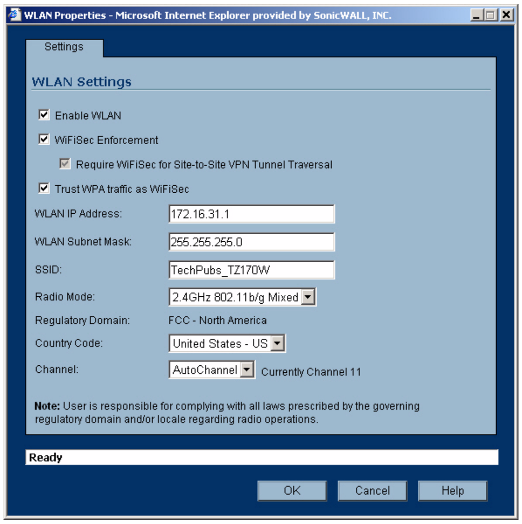
The SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless includes the **WLAN** interface in the **Interfaces** table on the **Network>Settings** page.



Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.25	255.255.0.0	100 Mbps, half duplex	
LAN		192.168.168.168	255.255.255.0	no link	
WLAN		172.16.31.1	255.255.255.0	0 Mbps, 802.11b/g Mixed	

Clicking the Edit icon for the **WLAN** interface displays the **WLAN Settings** window for configuring the WLAN properties.



WLAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings

WLAN Settings

☑ Enable WLAN
☑ WiFiSec Enforcement
☑ Require WiFiSec for Site-to-Site VPN Tunnel Traversal
☑ Trust WPA traffic as WiFiSec

WLAN IP Address: 172.16.31.1
WLAN Subnet Mask: 255.255.255.0
SSID: TechPubs_TZ170W
Radio Mode: 2.4GHz 802.11b/g Mixed
Regulatory Domain: FCC - North America
Country Code: United States - US
Channel: AutoChannel Currently Channel 11

Note: User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

Ready

- The **Enable WLAN** setting is checked by default to activate the WLAN interface on the SonicWALL security appliance.
- Select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN interface be either IPSec traffic, WPA traffic, or both. With **WiFiSec Enforcement** enabled, all non-guest wireless clients are required to use the strong security of IPSec. The VPN connection inherent in WiFiSec terminates at the GroupVPN Policy, which you can configure on the **VPN > Settings** page.
- If you have not selected **WiFiSec Enforcement**, you can select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a site-to-site VPN.
- Click **Trust WPA traffic** to accept WPA as an allowable alternative to IPSec. The SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless supports both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server).
- **WLAN IP Address**: The IP address of the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless WLAN interface.
- **WLAN Subnet Mask**: The subnet of the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless WLAN interface.

- **SSID**: Enter a recognizable string for the SSID for the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless security appliance. This is the name that will appear in clients' lists of available wireless connections.
- **Radio Mode**: The default 2.4GHZ 802.11b/g mixed enables the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support both 802.11b and 802.11g wireless card clients.
- **Country Code**: Select the country where you are operating the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. The country code determines which **Regulatory Domain** the radio operation falls under.
- **Channel**: Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use **AutoChannel** unless you have a specific reason to use or avoid specific channels.

CHAPTER

10

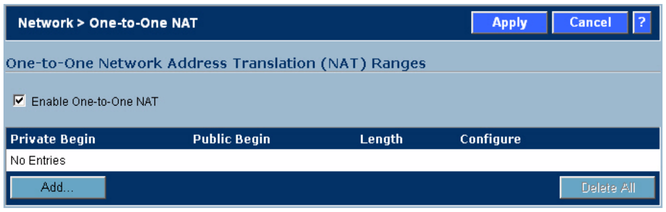
Configuring One-to-One NAT

Network > One-to-One NAT

One-to-One NAT maps valid, external addresses to private addresses hidden by NAT. Computers on your private LAN or OPT interface are accessed on the Internet at the corresponding public IP addresses.

You can create a relationship between internal and external addresses by defining internal and external address ranges. Once the relationship is defined, the computer with the first IP address of the private address range is accessible at the first IP address of the external address range, the second computer at the second external IP address, etc.

To configure One-to-One NAT, select the **Network > One-to-One NAT** page.


Network > One-to-One NAT
Apply
Cancel
?
One-to-One Network Address Translation (NAT) Ranges
Add...
Delete All

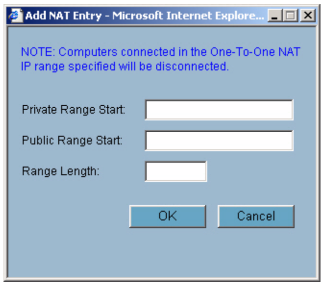
☑ Enable One-to-One NAT

Private Begin	Public Begin	Length	Configure
No Entries			

To configure One-to-One NAT, complete the following instructions.

1 Select the **Enable One-to-One NAT** check box.

2 Click **Add**. The **Add NAT Entry** window is displayed.


Add NAT Entry - Microsoft Internet Explore...
Private Range Start:
Public Range Start:
Range Length:
OK
Cancel

NOTE: Computers connected in the One-To-One NAT IP range specified will be disconnected.

3 Enter the beginning IP address of the private address range being mapped in the **Private Range Start** field. This is the IP address of the first machine that is accessible from the Internet.

4. Enter the beginning IP address of the valid address range being mapped in the **Public Range Begin** field. This address should be assigned by your ISP and be in the same logical subnet as the NAT public IP address.

Alert: *Do not include the SonicWALL security appliance WAN IP (NAT Public) Address or the WAN Gateway (Router) Address in this range.*

5. Enter the number of public IP addresses that should be mapped to private addresses in the Range Length field. The range length can not exceed the number of valid IP addresses. Up to 64 ranges can be added. To map a single address, enter a Range Length of 1.
6. Click **OK**.
7. Click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

Alert: *One-to-One NAT maps valid, public IP addresses to private LAN or OPT IP addresses. It does not allow traffic from the Internet to the private LAN.*

Tip: *After One-to-One NAT is configured, create an Allow rule to permit traffic from the Internet to the private IP address(es) on the LAN or OPT.*

To edit an existing entry in the One-to-One Network Address Translation (NAT) Ranges, click the edit icon. To delete an entry, click the delete icon. To delete all entries, click **Delete All**.

One-to-One NAT Configuration Example

This example assumes that you have a SonicWALL security appliance running in the NAT-enabled mode, with IP addresses on the LAN in the range 192.168.1.1 - 192.168.1.254, and a WAN IP address of 208.1.2.2. Also, you own the IP addresses in the range 208.1.2.1 - 208.1.2.6.

Alert: *If you have only one IP address from your ISP, you cannot use One-to-One NAT.*

You have three web servers on the LAN with the IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.12. Each of the servers must have a default gateway pointing to 192.168.1.1, the SonicWALL security appliance LAN IP address.

You also have three additional IP addresses from your ISP, 208.1.2.4, 208.1.2.5, and 208.1.2.6, that you want to use for three additional web servers. Use the following steps to configure One-to-One NAT:

1. Select **Enable One-to-One NAT**.
2. Click **Add**. The **Add NAT Entry** window is displayed
3. Enter in the IP address, 192.168.1.10, in the **Private Range Begin** field.
4. Enter in the IP address, 208.1.2.4, in the **Public Range Begin** field.
5. Enter in 3 in the **Range Length** field.

Tip: *You can configure the IP addresses individually, but it is easier to configure them in a range. However, the IP addresses on both the private and public sides must be consecutive to configure a range of addresses.*

6. Click **OK**.
7. Click **Apply**.
8. Click **Firewall**, then **Access Rules**.
9. Click **Add**.

10 Configure the following settings:

- **Allow**
- **Service** - HTTP
- **Source** - WAN
- **Destination** - LAN 192.168.1.10 - 192.168.1.12

In the **Options** tab, select **always** from the **Apply this Rule** menu.

11 Click **OK**.

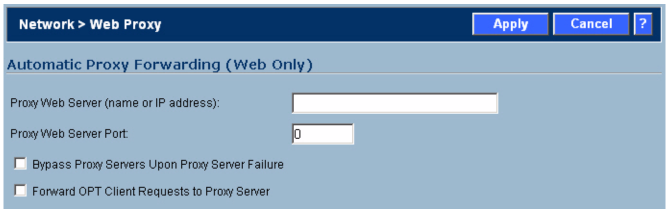
Requests for <http://208.1.2.4> are answered by the server at 192.168.1.10. Requests for <http://208.1.2.5> are answered by the server at 192.168.1.11, and requests for <http://208.1.2.6> are answered by the server at 192.168.1.12. From the LAN, the servers can only be accessed using the private IP addresses (192.168.1.x), not the public IP addresses or domain names. For example, from the LAN, you must use URLs like <http://192.168.1.10> to reach the web servers. An IP address, such as 192.168.1.10, on the LAN cannot be used in both public LAN server configurations and in public LAN server One-to-One NAT configurations.

CHAPTER

11

Configuring Web Proxy Settings

Network > Web Proxy



Automatic Proxy Forwarding (Web Only)

Proxy Web Server (name or IP address):

Proxy Web Server Port: 0

☐ Bypass Proxy Servers Upon Proxy Server Failure

☐ Forward OPT Client Requests to Proxy Server

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests.

Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN and enable Web Proxy Forwarding. The SonicWALL security appliance automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Configuring Automatic Web Proxy Forwarding

Alert: *The proxy server must be located on the WAN; it can not be located on the LAN.*

To configure a Proxy Web sever, select the **Network > Web Proxy** page.

1. Connect your Web proxy server to a hub, and connect the hub to the SonicWALL security appliance WAN port.
2. Enter the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
3. Enter the proxy IP port in the **Proxy Web Server Port** field.
4. To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
5. To send proxy requests from the OPT interface as well as the LAN interface, check the **Forward OPT/DMZ/WLAN Client Requests to Proxy Server** checkbox.
6. Click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Network > Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL security appliance to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

Forward OPT/DMZ/WLAN Client Requests to Proxy Server

By default, client requests coming in through the OPT interface are not forwarded to the Proxy Server. To send OPT/DMZ/WLAN client requests as well as LAN client requests, check the **Forward OPT/DMZ/WLAN Client Requests to Proxy Server** checkbox.

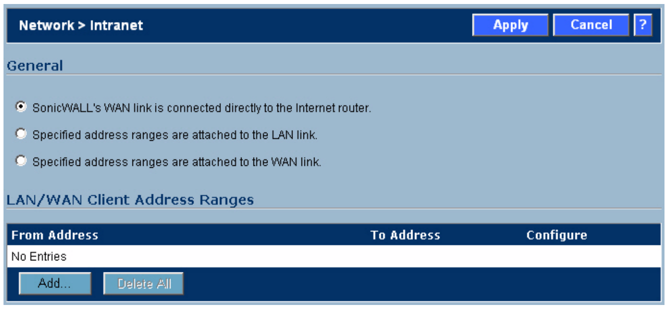
CHAPTER

12

Configuring Intranet Settings

Network > Intranet

The SonicWALL security appliance can be configured as an Intranet firewall to prevent network users from accessing sensitive servers. By default, users on your LAN can access the Internet router, but not devices connected to the WAN port of the SonicWALL security appliance. To enable access to the area between the SonicWALL security appliance WAN port and the Internet, you must configure the Intranet settings on the SonicWALL security appliance on the **Network > Intranet** page.



● SonicWALL's WAN link is connected directly to the Internet router.
○ Specified address ranges are attached to the LAN link.
○ Specified address ranges are attached to the WAN link.

From Address	To Address	Configure
No Entries		

Intranet firewalling is achieved by connecting the SonicWALL security appliance between an unprotected and a protected segment, as shown below.

Installation

1. Connect the LAN Ethernet port on the back of the SonicWALL security appliance to the network segment to be protected against unauthorized access.

Alert: *Devices connected to the WAN port do not have firewall protection. It is recommended that you use another SonicWALL security appliance to protect computers on the WAN.*

2. Connect the SonicWALL security appliance to a power outlet and make sure the SonicWALL security appliance is powered on.

To enable an Intranet firewall, you must specify which machines are located on the LAN, or you must specify which machines are located on the WAN.

It is best to select the network area with the least number of machines. For example, if only one or two machines are connected to the WAN, select **Specified address ranges are attached to the WAN link**. That way, you only have to enter one or two IP addresses in the **Add Range** section. Specify the IP addresses individually or as a range.

Intranet Settings

1. In the left-navigation menu, select **Network** and then **Intranet**.
2. Select one of the following options:

- **SonicWALL WAN link is connected directly to the Internet router**

  Select this option if the SonicWALL security appliance is protecting your entire network. This is the default setting.

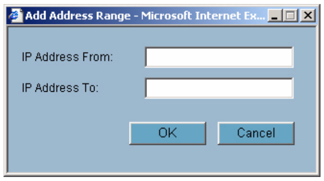
- **Specified address ranges are attached to the LAN link**

  Select this option if it is easier to specify the devices on your LAN. Then enter your LAN IP address range(s). If you do not include all computers on your LAN, the computers not included will be unable to send or receive data through the SonicWALL security appliance.

- **Specified address ranges are attached to the WAN link**

  Select this option if it is easier to specify the devices on your WAN. Then enter your WAN IP address range(s). Computers connected to the WAN port that are not included are inaccessible to users on your LAN.

3. Click **Add** to add a specific range of IP addresses on your LAN or OPT interfaces to include in your Intranet. Clicking **Add** displays the **Add Address Range** window. To add a range of addresses, such as “199.2.23.50” to “199.2.23.54”, enter the starting address in the **From Address** field and the ending address in the **To Address** field. An individual IP address should be entered in the **From Address** field only.



Tip: *Up to 64 address ranges can be entered.*

4. Click **Update**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

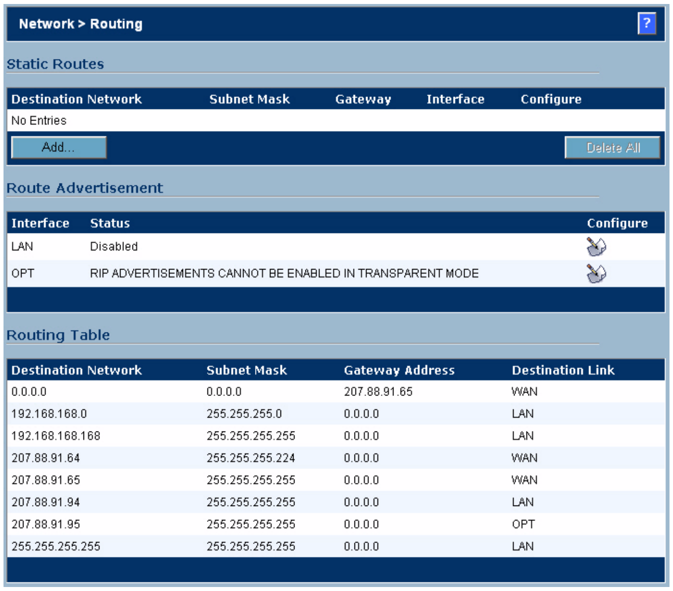
CHAPTER

13

Configuring Static Routes

Network > Routing

If you have routers on your LAN or WAN, you can configure static routes on the SonicWALL security appliance using the settings on the **Network > Routing** page.



Network > Routing

Static Routes

Destination Network	Subnet Mask	Gateway	Interface	Configure
No Entries				

Route Advertisement

Interface	Status	Configure
LAN	Disabled	
OPT	RIP ADVERTISEMENTS CANNOT BE ENABLED IN TRANSPARENT MODE	

Routing Table

Destination Network	Subnet Mask	Gateway Address	Destination Link
0.0.0.0	0.0.0.0	207.88.91.65	WAN
192.168.168.0	255.255.255.0	0.0.0.0	LAN
192.168.168.168	255.255.255.255	0.0.0.0	LAN
207.88.91.64	255.255.255.224	0.0.0.0	WAN
207.88.91.65	255.255.255.255	0.0.0.0	WAN
207.88.91.94	255.255.255.255	0.0.0.0	LAN
207.88.91.95	255.255.255.255	0.0.0.0	OPT
255.255.255.255	255.255.255.255	0.0.0.0	LAN

Static routing means configuring the SonicWALL security appliance to route network traffic to a specific, predefined destination. Static routes must be defined if the LAN or WAN are segmented into subnets, either for size or practical considerations. For example, a subnet can be created to isolate a section of a company, such as finance, from network traffic on the rest of the LAN or WAN.

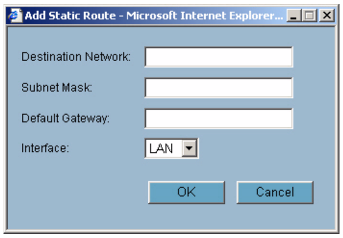
Static Routes

Static Routes are configured when network traffic is directed to subnets located behind routers on your network. For instance, you have a router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 - 10.0.5.254 with a subnet mask of 255.255.255.0. You can configure static routes on the LAN, WAN, DMZ, OPT, and WLAN interfaces.

To configure a static route to the 10.0.5.0 subnet, follow these instructions:

1 Click **Network**, then **Routing**.

2 Click **Add** in the **Static Routes** section. The **Add Static Route** window is displayed.



Interface: LAN

3 Enter 10.0.5.0 in the **Destination Network** field.

4 Enter 255.255.255.0 in the **Subnet Mask** field.

5 Enter 192.168.168.254 in the **Default Gateway** field. This is the IP address of the router.

6 Select **LAN** from the **Interface** menu.

7 Click **OK.**

✓ **Tip:** *You can configure up to 256 routes on the SonicWALL security appliance.*

Static Route Configuration Example

Static Route configurations allow for multiple subnets separated by an internal (LAN) router to be supported behind the SonicWALL security appliance LAN. This option is only be used when the secondary subnet is accessed through an internal (LAN) router that is between it and the SonicWALL security appliance LAN port. Once static routes are configured, network traffic can be directed to these subnets.

Key terms:

- **Destination Network**: the network IP address of the remote subnet. The address usually ends in 0, i.e 10.0.5.0.
- **Subnet Mask**: the subnet mask of the remote network (i.e. 255.255.255.0)
- **Gateway**: the IP address of the Internal (LAN) router that is local to the SonicWALL security appliance.

For example:

SonicWALL LAN IP Address: 192.168.168.1
Subnet mask: 255.255.255.0
Router IP Address: 192.168.168.254
Secondary Subnet: 10.0.5.0
Subnet mask: 255.255.255.0

If you have an Internal (LAN) router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 - 10.0.5.254 with a subnet mask of 255.255.255.0. To configure a static route to the 10.0.5.0 subnet, follow these instructions:

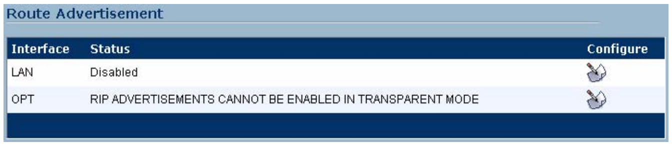
Click **Network**, and then **Routing**.

1. Click **Add** in the **Static Routes** section.
2. Enter 10.0.5.0 in the **Destination Network** field.
3. Enter 255.255.255.0 in the **Subnet Mask** field.
4. Enter 192.168.168.254 in the **Default Gateway** field. This is the IP address of the internal (LAN) router that is local to the SonicWALL security appliance.
5. Select **LAN** from the **Interface** menu.
6. Click **OK**.

✓ **Tip:** *Be sure the Internal (LAN) router is configured as follows: If the SonicWALL security appliance is in NAT Enabled mode, the internal (LAN) router needs to have a route of last resort (i.e. gateway address) that is the SonicWALL security appliance LAN IP address.*

Route Advertisement

The SonicWALL security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.



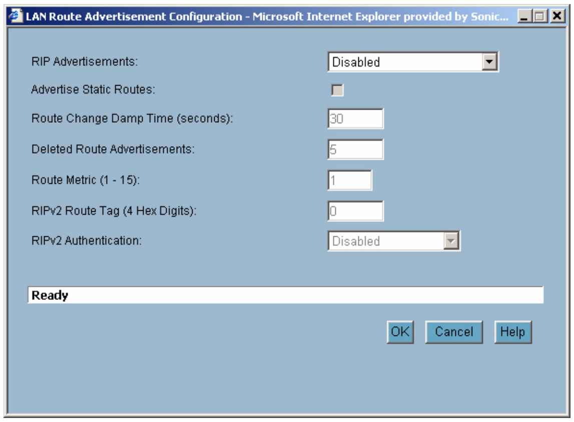
Route Advertisement

Interface	Status	Configure
LAN	Disabled	✎
OPT	RIP ADVERTISEMENTS CANNOT BE ENABLED IN TRANSPARENT MODE	✎

Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

1. Click the edit icon ✎ in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.



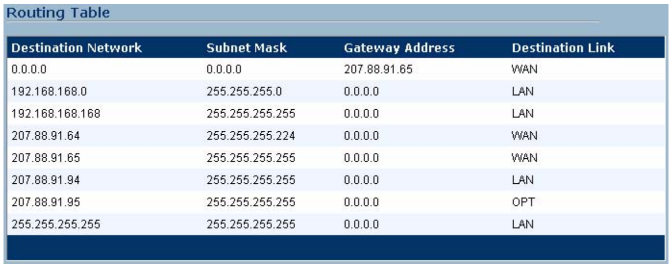
LAN Route Advertisement Configuration - Microsoft Internet Explorer provided by Sonic...

RIP Advertisements: Disabled
Advertise Static Routes: ☐
Route Change Damp Time (seconds): 30
Deleted Route Advertisements: 5
Route Metric (1 - 15): 1
RIPv2 Route Tag (4 Hex Digits): 0
RIPv2 Authentication: Disabled

Ready

2. Select one of the following types of RIP Advertisements:
   - **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
   - **RIPv2 Enabled (multicast)** - to send route advertisements using multicasting (a single data packet to specific notes on the network).
   - **RIPv2 Enabled (broadcast)** - to send route advertisements using broadcasting (a single data packet to all nodes on the network).
3. Enable **Advertise Static Routes** if you have static routes configured on the SonicWALL security appliance, enable this feature to exclude them from Route Advertisement.
4. Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds**) field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds**) setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.
5. Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99**) field. The default value is **1**.
6. Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.
7. If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.
8. If you wan to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:
   - **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
   - **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.
   - **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.
9. Click **OK**.

Routing Table



Routing Table

Destination Network	Subnet Mask	Gateway Address	Destination Link
0.0.0.0	0.0.0.0	207.88.91.65	WAN
192.168.168.0	255.255.255.0	0.0.0.0	LAN
192.168.168.168	255.255.255.255	0.0.0.0	LAN
207.88.91.64	255.255.255.224	0.0.0.0	WAN
207.88.91.65	255.255.255.255	0.0.0.0	WAN
207.88.91.94	255.255.255.255	0.0.0.0	LAN
207.88.91.95	255.255.255.255	0.0.0.0	OPT
255.255.255.255	255.255.255.255	0.0.0.0	LAN

The **Routing Table** is a list of destinations that the IP software maintains on each host and router.

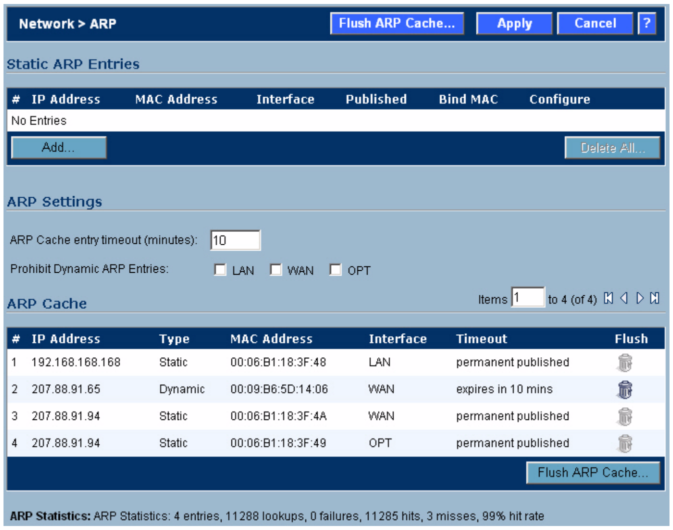
The network IP address, subnet mask, gateway address, and the corresponding link are displayed.

Most of the entries are the result of configuring LAN, WAN, and OPT network settings. The SonicWALL security appliance LAN, WAN, and OPT IP addresses are displayed as permanently published at all times.

CHAPTER 14

Configuring Address Resolution Protocol Settings

Network > ARP



Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
No Entries						

ARP Settings

ARP Cache entry timeout (minutes): 10

Prohibit Dynamic ARP Entries: ☐ LAN ☐ WAN ☐ OPT

ARP Cache

Items 1 to 4 (of 4)

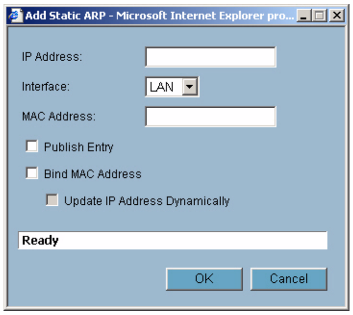
#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	192.168.168.168	Static	00:06:B1:18:3F:48	LAN	permanent published	
2	207.88.91.65	Dynamic	00:09:B6:5D:14:06	WAN	expires in 10 mins	
3	207.88.91.94	Static	00:06:B1:18:3F:4A	WAN	permanent published	
4	207.88.91.94	Static	00:06:B1:18:3F:49	OPT	permanent published	

ARP Statistics: ARP Statistics: 4 entries, 11288 lookups, 0 failures, 11285 hits, 3 misses, 99% hit rate

The ARP (Address Resolution Protocol) Cache stores IP or logical addresses received from ARP replies in order to minimize the number of ARP broadcasts on a network. ARP broadcasts can degrade network performance if too many broadcast requests are sent over the network. Once the ARP request is stored, the host does not have to send out ARP requests for the same IP datagram.

Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:



Add Static ARP - Microsoft Internet Explorer pro...

IP Address:

Interface: LAN

MAC Address:

☐ Publish Entry

☐ Bind MAC Address

☐ Update IP Address Dynamically

Ready

- **Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the SonicWALL device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the SonicWALL device reply for a secondary IP address on a particular interface by adding the MAC address of the SonicWALL. See the Secondary Subnet section that follows.
- **Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only the used on a specified interface on the SonicWALL. Once the MAC address is bound to an interface, the SonicWALL will not respond to that MAC address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.
- **Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the Add Static ARP window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP Address allocated by the SonicWALL's internal DHCP server, or by the external DHCP server if IP Helper is in use.

Secondary Subnets with Static ARP

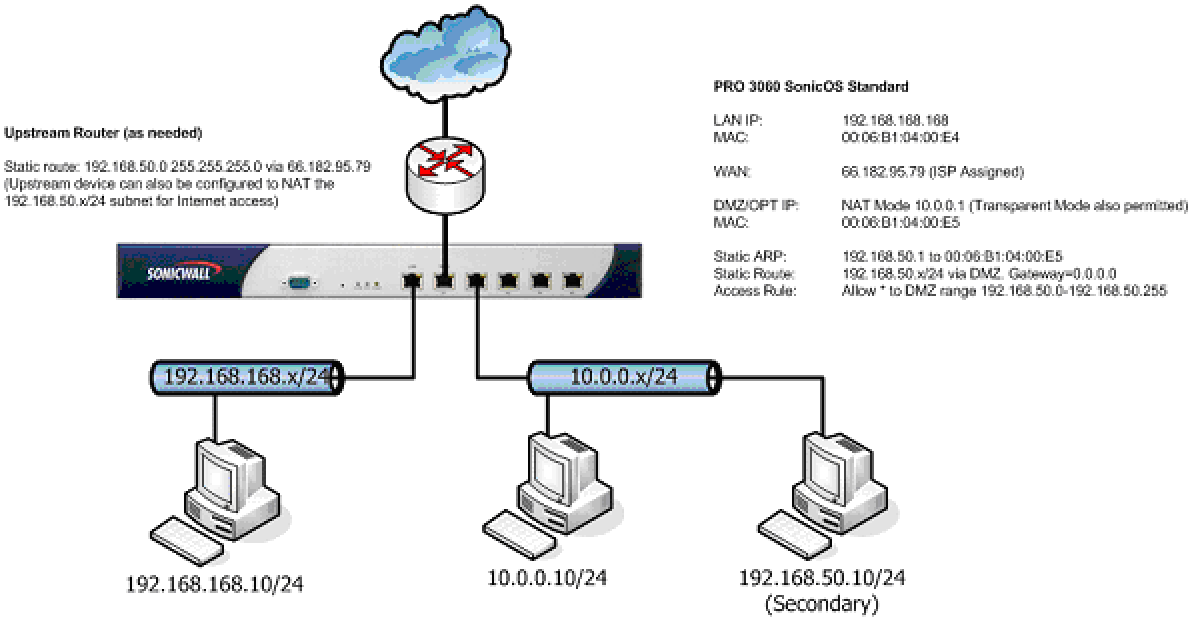
SonicOS Standard already supports secondary subnets on the LAN using the **Network Gateway** feature on LAN Properties window from the **Network > Settings** page, but the Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

Note: *It is not possible to create firewall access rules between primary and secondary subnets, when they are created using the static ARP method.*

Adding a Secondary Subnet using the Static ARP Method

1. Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the SonicWALL interface to which it will be connected.
2. Add a static route for that subnet, so that the SonicWALL regards it as valid traffic, and knows to which interface to route that subnet's traffic.
3. Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.
4. Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:



Upstream Router (as needed)

Static route: 192.168.50.0 255.255.255.0 via 66.182.95.79
(Upstream device can also be configured to NAT the
192.168.50.x/24 subnet for Internet access)

PRO 3060 SonicOS Standard

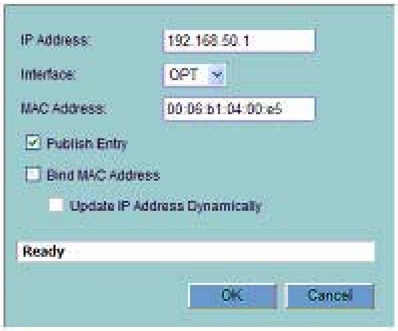
LAN IP: 192.168.168.168
MAC: 00:06:B1:04:00:E4

WAN: 66.182.95.79 (ISP Assigned)

DMZ/OPT IP: NAT Mode 10.0.0.1 (Transparent Mode also permitted)
MAC: 00:06:B1:04:00:E5

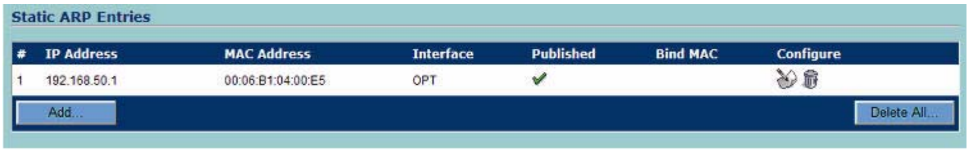
Static ARP: 192.168.50.1 to 00:06:B1:04:00:E5
Static Route: 192.168.50.x/24 via DMZ. Gateway=0.0.0.0
Access Rule: Allow * to DMZ range 192.168.50.0-192.168.50.255

With SonicOS Standard, although it is not possible to create a NAT rule for a secondary subnet on the DMZ (or OPT) interface, it is possible to support the secondary subnet in a routed configuration. To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the DMZ/OPT interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:



IP Address: 192.168.50.1
Interface: OPT
MAC Address: 00:06:b1:04:00:e5
☑ Publish Entry
☐ Bind MAC Address
☐ Update IP Address Dynamically
Ready

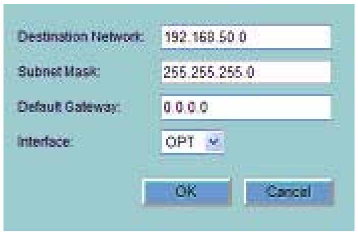
The entry will appear in the table as follows:



Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
1	192.168.50.1	00:06:B1:04:00:E5	OPT	✓		

Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network as follows:



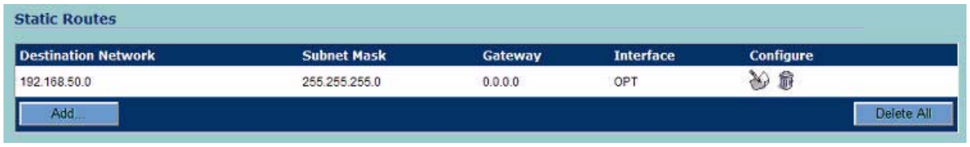
Destination Network: 192.168.50.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Interface: OPT

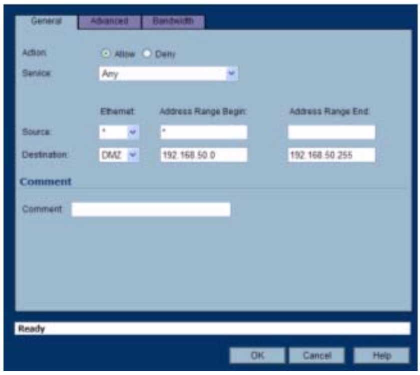
The entry will appear in the table as follows:



Static Routes

Destination Network	Subnet Mask	Gateway	Interface	Configure
192.168.50.0	255.255.255.0	0.0.0.0	OPT	

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add the following Access Rule:



Action: ● Allow ○ Deny

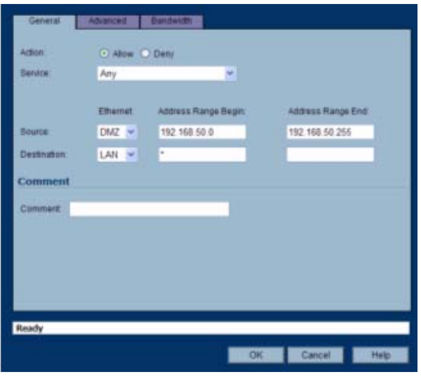
Service: Any

	Ethernet:	Address Range Begin:	Address Range End:
Source:	*	*	
Destination:	DMZ	192.168.50.0	192.168.50.255

Comment

Comment:

Ready



Action: ● Allow ○ Deny

Service: Any

	Ethernet:	Address Range Begin:	Address Range End:
Source:	DMZ	192.168.50.0	192.168.50.255
Destination:	LAN	*	

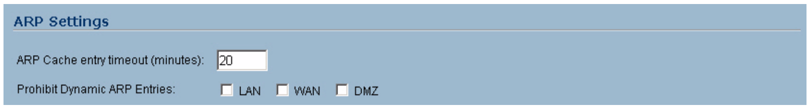
Comment

Comment:

Ready

Prohibit Dynamic ARP Entries

SonicOS Standard provides the ability to prohibit dynamic ARP entries on a per-interface basis. Enabling this feature on an interface will prevent that interface from dynamically adding ARP entries. This is offered as a security mechanism to statically and strictly define the MAC addresses of hosts that will be permitted to operate on a particular interface.



ARP Settings

ARP Cache entry timeout (minutes): 20

Prohibit Dynamic ARP Entries: ☐ LAN ☐ WAN ☐ DMZ

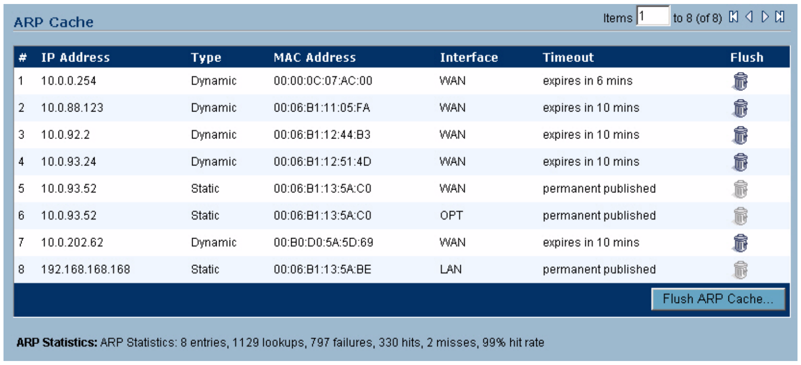
▲ **Alert:** *Misuse or misconfiguration of this feature can render the SonicWALL inaccessible and recoverable only by restoring factory defaults. Be certain to understand the behavior of this feature, and to have properly configured static ARP entries for allowed hosts prior to applying any 'prohibit dynamic ARP entry' settings.*

A typical use for this feature would be prohibiting dynamic ARP on the WAN interface, after adding a static ARP entry for the upstream router. This will help to ensure that the router will be the only host allowed on the WAN interface.

After adding the static ARP entry for the router, mark the checkbox next to the WAN interface in the 'Prohibit dynamic ARP entries' area. Click the **OK** button in the alert dialog to proceed. The setting will not take effect until the **Apply** button at the top of the page is selected.

Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table.



#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	10.0.0.254	Dynamic	00:00:0C:07:AC:00	WAN	expires in 6 mins	
2	10.0.88.123	Dynamic	00:06:B1:11:05:FA	WAN	expires in 10 mins	
3	10.0.92.2	Dynamic	00:06:B1:12:44:B3	WAN	expires in 10 mins	
4	10.0.93.24	Dynamic	00:06:B1:12:51:4D	WAN	expires in 10 mins	
5	10.0.93.52	Static	00:06:B1:13:5A:C0	WAN	permanent published	
6	10.0.93.52	Static	00:06:B1:13:5A:C0	OPT	permanent published	
7	10.0.202.62	Dynamic	00:B0:D0:5A:5D:69	WAN	expires in 10 mins	
8	192.168.168.168	Static	00:06:B1:13:5A:BE	LAN	permanent published	

ARP Statistics: ARP Statistics: 8 entries, 1129 lookups, 797 failures, 330 hits, 2 misses, 99% hit rate

Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP Cache** to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.

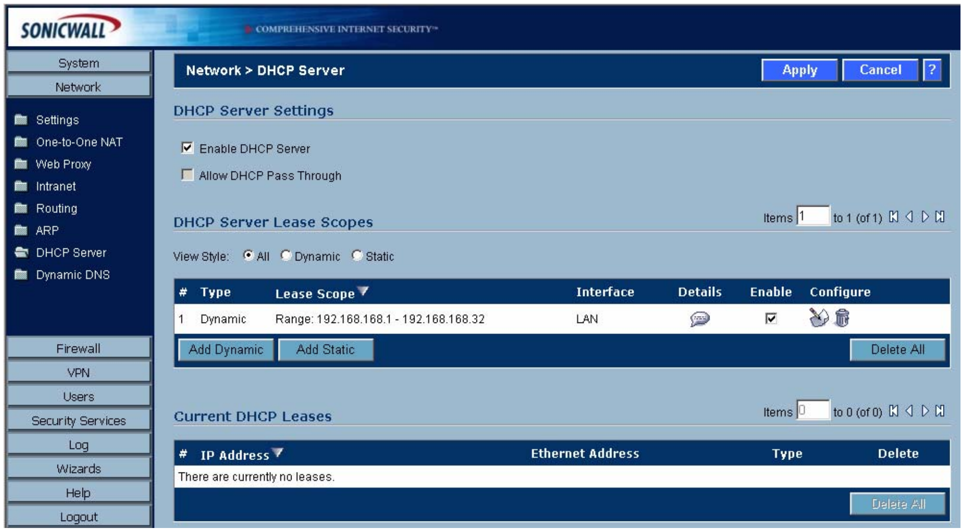
CHAPTER

15

Configuring the DHCP Server

Network > DHCP Server

The SonicWALL security appliance DHCP Server distributes IP addresses, subnet masks, gateway addresses, and DNS server addresses to the computers on your network. You can use the SonicWALL DHCP server or another DHCP server on your network.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Dynamic DNS
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Network > DHCP Server
Apply
Cancel
?
Add Dynamic
Add Static
Delete All
Delete All

DHCP Server Settings

☑ Enable DHCP Server

☐ Allow DHCP Pass Through

DHCP Server Lease Scopes

Items 1 to 1 (of 1)

View Style: ● All ○ Dynamic ○ Static

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 192.168.168.1 - 192.168.168.32	LAN		☑	

Current DHCP Leases

Items 0 to 0 (of 0)

#	IP Address	Ethernet Address	Type	Delete
There are currently no leases.				

DHCP Server Settings

To enable the DHCP server feature on the SonicWALL security appliance, select **Enable DHCP Server**.

To use another DHCP server on your network, uncheck **Enable DHCP Server**.

Select **Allow DHCP Pass Through** is you are using another DHCP server on your network.

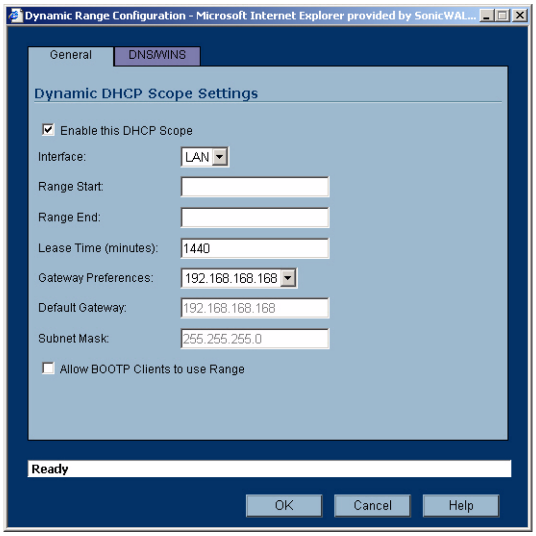
DHCP Server Lease Scopes

The DHCP **Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type**: **Dynamic** or **Static**
- **Lease Scope**: The IP address range, for example **172.16.31.2 - 172.16.31.254**
- **Interface**: The Interface the range is assigned to **LAN**, **OPT**, **DMZ, WLAN** or **WAN**
- **Details**: Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the details icon
- **Enable**: Check the box in the **Enable** column to enable the DHCP range. Uncheck it to disable the range
- **Configure**: Click the edit icon to configure the DHCP range or the delete icon to delete the scope

Configuring DHCP Server for Dynamic Ranges

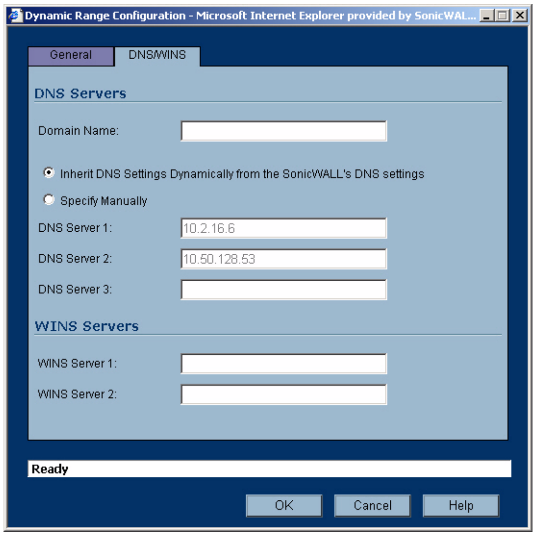
1. Click the **Add Dynamic** button. The **Dynamic Range Configuration** window is displayed.


Dynamic Range Configuration - Microsoft Internet Explorer provided by SonicWAL...
General
DNS/WINS
Dynamic DHCP Scope Settings
Ready
OK
Cancel
Help

☑ Enable this DHCP Scope
Interface: LAN
Range Start:
Range End:
Lease Time (minutes): 1440
Gateway Preferences: 192.168.168.168
Default Gateway: 192.168.168.168
Subnet Mask: 255.255.255.0
☐ Allow BOOTP Clients to use Range

2. Make sure the **Enable this DHCP Scope** is checked if you want this DHCP scope enable after you click **OK**.
3. Select the interface from the **Interface** menu. The IP addresses are in the same private subnet as the SonicWALL security appliance LAN.
4. Enter the beginning IP address in the **Range Start** field. The default IP address is appropriate for most networks.
5. Enter the last IP address in the **Range End** field. If there are more than 25 computers on your network, enter the appropriate ending IP address in the **Range End** field.
6. Enter the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes is the default value.
7. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and enter a different IP address for the gateway.
8. If you select the SonicWALL security appliance LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to enter the Default Gateway and Subnet Mask information into the fields.
9. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

10 Click the **DNS/WINS** tab to continue configuring the DHCP server.


Dynamic Range Configuration - Microsoft Internet Explorer provided by SonicWAL...
General
DNS/WINS
DNS Servers
WINS Servers
Ready
OK
Cancel
Help

Domain Name:

● Inherit DNS Settings Dynamically from the SonicWALL's DNS settings

○ Specify Manually

DNS Server 1: 10.2.16.6

DNS Server 2: 10.50.128.53

DNS Server 3:

WINS Server 1:

WINS Server 2:

11 If you have a domain name for the DNS Server, enter it in the **Domain Name** field.

12 **Inherit DNS Settings Dynamically from the SonicWALL's DNS Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

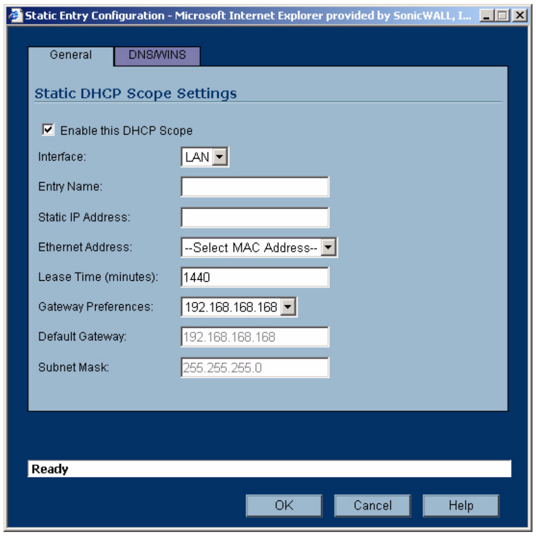
13 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and enter the IP address of your DNS Server in the **DNS Server** fields.

14 If you have WINS running on your network, enter the WINS server IP address(es) in the **WINS Server** fields.

15 Click **OK** to add the settings to the SonicWALL security appliance. Then click **Apply** for the settings to take effect on the SonicWALL security appliance.

Configuring Static DHCP Entries

1 Click the **Add Static** button. The **Static Entry Configuration** window is displayed.


Static Entry Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
General
DNS/WINS
Static DHCP Scope Settings
Ready
OK
Cancel
Help

☑ Enable this DHCP Scope

Interface: LAN

Entry Name:

Static IP Address:

Ethernet Address: --Select MAC Address--

Lease Time (minutes): 1440

Gateway Preferences: 192.168.168.168

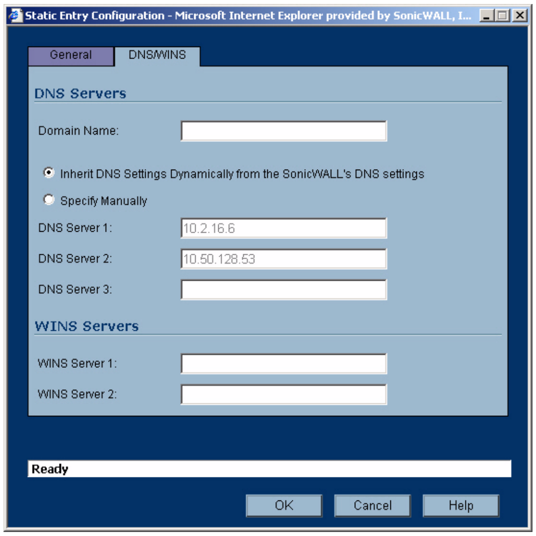
Default Gateway: 192.168.168.168

Subnet Mask: 255.255.255.0

2 Make sure the **Enable this DHCP Scope** is checked if you want this DHCP scope enable after you click **OK**.

3 Select the interface from the **Interface** menu. The IP addresses are in the same private subnet as the SonicWALL security appliance LAN.

4. Enter the device IP address in the **Static IP Address** field.
5. Enter the device Ethernet (MAC) address in the **Ethernet Address** field.
6. Enter the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes is the default value.
7. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and enter a different IP address for the gateway.
8. If you select the SonicWALL security appliance LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to enter the Default Gateway and Subnet Mask information into the fields.
9. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.
10. Click the **DNS/WINS** tab to continue configuring the DHCP server.


Static Entry Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
General
DNS/WINS
OK
Cancel
Help

DNS Servers

Domain Name:

● Inherit DNS Settings Dynamically from the SonicWALL's DNS settings

○ Specify Manually

DNS Server 1: 10.2.16.6

DNS Server 2: 10.50.128.53

DNS Server 3:

WINS Servers

WINS Server 1:

WINS Server 2:

Ready

11. If you have a domain name for the DNS Server, enter it in the **Domain Name** field.
12. **Inherit DNS Settings Dynamically from the SonicWALL's DNS Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.
13. If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and enter the IP address of your DNS Server in the **DNS Server** fields. You must specify at least one DNS server.
14. If you have WINS running on your network, enter the WINS server IP address(es) in the **WINS Server** fields.
15. Click **OK** to add the settings to the SonicWALL security appliance. Then click **Apply** for the settings to take effect on the SonicWALL security appliance.

✓ **Tip:** *The SonicWALL security appliance DHCP server can assign a total of 254 dynamic and static IP addresses.*

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding displays the IP address and the Ethernet address along with the type of binding, Dynamic, Dynamic BOOTP, or Static BOOTP. To delete a binding, which frees the IP address on the DHCP server, click the Trashcan icon next to the entry. To edit an entry, click the edit icon next to the entry.

CHAPTER 16

Configuring Dynamic DNS

Network > Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, is a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. SonicWALL does not provide technical support for DDNS providers - the providers themselves must be contacted.

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS 3.0 currently supports the following services from four Dynamic DNS providers:

- Dyndns.org <http://www.dyndns.org> - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- Changeip.com <http://www.changeip.com> - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- No-ip.com <http://www.no-ip.com> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- Yi.org <http://www.yi.org> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

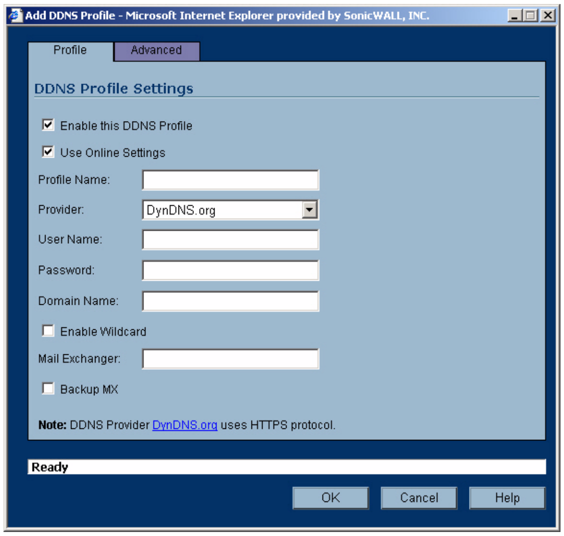
- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, e.g. server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

Configuring Dynamic DNS

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email.

After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS.

1. From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.


Add DDNS Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
Profile
Advanced
OK
Cancel
Help

DDNS Profile Settings

☑ Enable this DDNS Profile

☑ Use Online Settings

Profile Name:

Provider: DynDNS.org

User Name:

Password:

Domain Name:

☐ Enable Wildcard

Mail Exchanger:

☐ Backup MX

Note: DDNS Provider DynDNS.org uses HTTPS protocol.

Ready

2. If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the SonicWALL security appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.
3. If **Use Online Settings** is checked, the profile is administratively online.
4. Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.
5. In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. This example uses *DynDNS.org*. Dyndns.org requires the selection of a service. This example assumes you have created a dynamic service record with dyndns.org.
6. Enter your dyndns.org username and password in the **Username** and **Password** fields.
7. Enter the fully qualified domain name (FQDN) of the hostname you registered with dyndns.org. Make sure you provide the same hostname and domain as you configured.
8. You may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field.
9. Click the **Advanced** tab. You can typically leave the default settings on this page.
10. The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

    Let the server detect IP Address - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.

    Automatically set IP Address to the Primary WAN Interface IP Address - This will cause the SonicWALL device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.

Specify IP Address manually - Allows for the IP address to be registered to be manually specified and asserted.

11 The **Off-line Settings** section controls what IP Address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWALL. The options are:

Do nothing - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.

Use the Off-Line IP Address previously configured at Providers site - If your provider supports manual configuration of **Off-Line Settings**, you can select this option to use those settings when this profile is taken administratively offline.

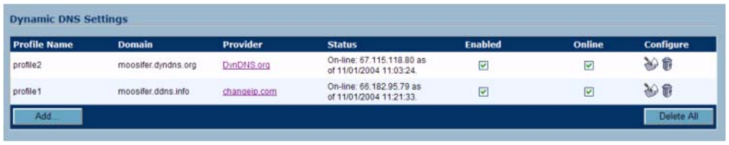
Make Host Unknown - De-registers the entry altogether. This action may take time to propagate through the DNS system.

Specify IP Address manually - Allows for an alternative address to be registered in the even that the entry is taken off-line.

12 Click **OK**.

Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.



Dynamic DNS Settings

Profile Name	Domain	Provider	Status	Enabled	Online	Configure
profile2	moosifer.dyndns.org	DynDNS.org	On-line: 67.115.118.80 as of 11/01/2004 11:03:24.	☑	☑	
profile1	moosifer.ddns.info	changeip.com	On-line: 66.182.95.79 as of 11/01/2004 11:21:33.	☑	☑	

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
  - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
  - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
  - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
  - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
  - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
  - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
  - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
  - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
  - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the SonicWALL will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the SonicWALL will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the edit icon for configuring the DDNS profile settings, and the delete icon for deleting the DDNS profile entry.

PART
4

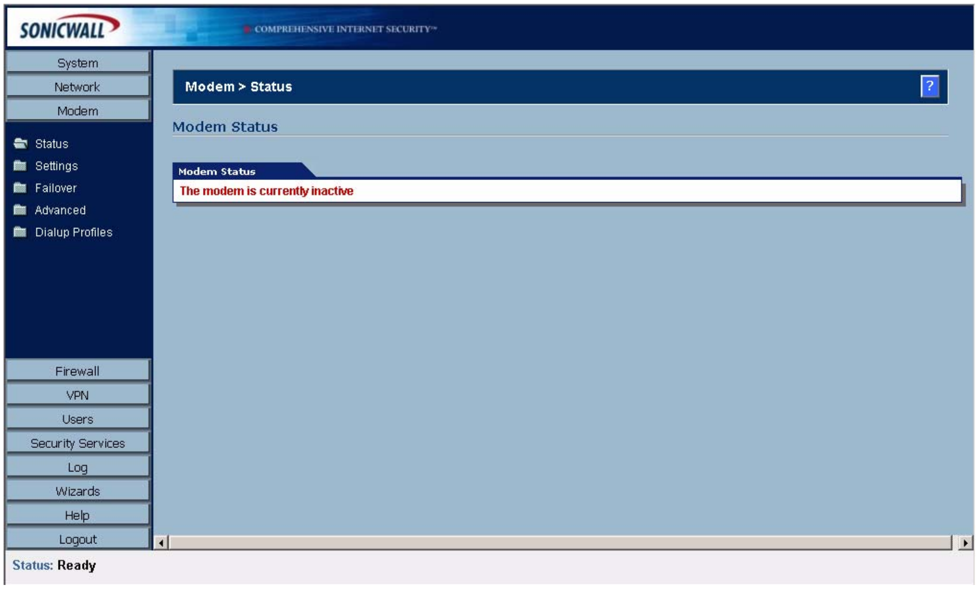
Modem

CHAPTER 17

Viewing Modem Status

Modem > Status

The **Status** page displays dialup connection information when the modem is active. You create modem dialup profiles in the **Modem Profile Configuration** window, which you access from the **Modem>Dialup Profiles** page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Modem
Status
Settings
Failover
Advanced
Dialup Profiles
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Modem > Status
?
Modem Status
Modem Status

The modem is currently inactive

Status: Ready

Modem Status

In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access. If you select the **Modem >Settings** page, a message is displayed reminding you that the modem is active and the current network settings are displayed on the **Modem >Status** page.

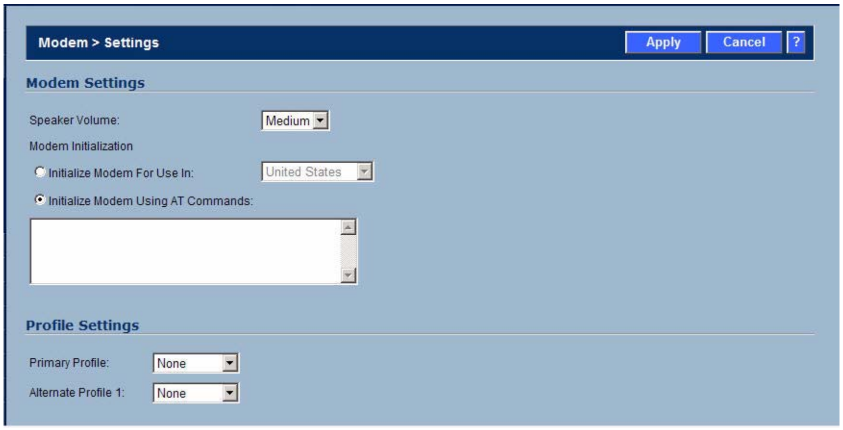
CHAPTER

18

Configuring Modem Settings

Modem > Settings

The **Modem > Settings** page lets you select from a list of modem profiles, select the volume of the modem, and also configure AT commands for modem initialization.


Modem > Settings
Apply
Cancel
?
Modem Settings
Profile Settings

Speaker Volume: Medium

Modem Initialization

○ Initialize Modem For Use In: United States

● Initialize Modem Using AT Commands:

Primary Profile: None

Alternate Profile 1: None

Configuring Profile and Modem Settings

To configure the SonicWALL security appliance modem settings, perform the following steps:

1. Select the volume of the modem from the **Speaker Volume** menu. The default value is **Medium**.
2. Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default.
3. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands** (**for modem initialization**) field. AT commands are instructions used to control a modem such as ATS7=30 (allows up to 30 seconds to wait for a dial tone), ATS8=2 (sets the amount of time the modem pauses when it encounters a “,” in the string).
4. Select the profile you want to use for the primary profile from the **Primary Profile** menu that the SonicWALL security appliance uses to access the modem. If you have enabled **Manual Dial** for the **Primary Profile**, the **Alternate Profile 1** is not used.
5. Select the secondary profile from the **Alternate Profile 1** menu. If the **Primary Profile** cannot establish a connection, the SonicWALL security appliance uses the **Alternate Profile 1** profile to access the modem and establish a connection

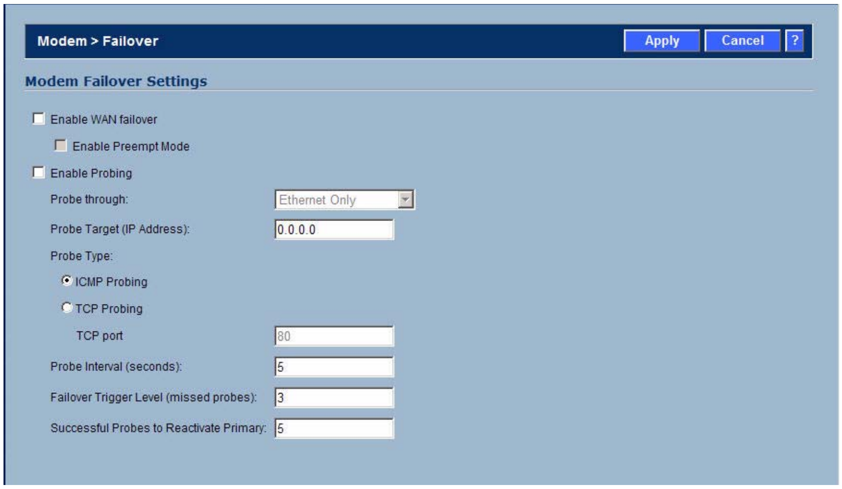
✓ **Tip:** *The default settings for the modem are generally sufficient for normal operation. The AT Commands (for modem initialization) box is provided for nonstandard situations.*

CHAPTER 19

Configuring Modem Failover

Modem > Failover

To improve the operational availability of networks and ensure fast recovery from network failures, the **Modem > Failover** page allows you to configure the SonicWALL security appliance modem for use as a secondary WAN port. The secondary WAN port can be used in a simple “active/passive” setup to allow traffic to be only routed through the secondary WAN port if the primary WAN port is unavailable. This allows the SonicWALL security appliance to maintain a persistent connection for WAN port traffic by “failing over” to the secondary WAN port.



Modem Failover Settings

☐ Enable WAN failover
☐ Enable Preempt Mode
☐ Enable Probing
Probe through: Ethernet Only
Probe Target (IP Address): 0.0.0.0
Probe Type:
● ICMP Probing
○ TCP Probing
TCP port 80
Probe Interval (seconds): 5
Failover Trigger Level (missed probes): 3
Successful Probes to Reactivate Primary: 5

Alert: *Using the WAN failover feature may cause disruption of some features such as One-to-One NAT. See the SonicWALL Administrator's Guide for affected features.*

After configuring your computer on the LAN, you can configure the SonicWALL security appliance modem connection for ISP failover or as a primary dial-up access port.

Modem Failover Settings

When you select **Enable WAN Failover**, the SonicWALL security appliance modem is used as a failover option when your “always on” DSL or cable connection fails. The SonicWALL security appliance automatically detects the failure of the WAN connection and uses the parameters configured for the modem in the Modem>Settings page.

Before you configure your **Modem Failover Settings**, create your dialup profiles in the Modem Profile Configuration window, which you access from the **Modem > Dialup Profiles** page.

▲ **Alert:** *The SonicWALL security appliance modem can only dial out. Dialling into the internal modem is not supported. However, an external modem can be connected to the* ***Console*** *port for remotely accessing the SonicWALL security appliance for out-of-band support.*

Configuring Modem Failover

Use the following instructions to configure the **Failover Settings**:

1. Select **Enable WAN Failover**.
2. Select **Enable Pre-empt Mode** if you want the primary WAN Ethernet interface to take over from the secondary modem WAN interface when it becomes active after a failure. If you do not enable **Pre-empt Mode**, the secondary WAN modem interface remains active as the WAN interface until you click **Disconnect**.
3. Select **Enable Probing**. Probing for WAN connectivity occurs over the Ethernet connection, the dial-up connection, or both. When probing is disabled on the Ethernet link, the SonicWALL security appliance only performs link detection. If the Ethernet connection is lost for a duration of 5-9 seconds, the SonicWALL security appliance considers the Ethernet connection to be unavailable. If the Ethernet link is lost for 0-4 seconds, the SonicWALL security appliance does not consider the connection to be lost. If you are swapping cables quickly, unnecessary WAN failover does not occur on the SonicWALL security appliance. If probing is enabled and the cable is unplugged, the 5-9 seconds link detection does not occur. Instead, the probing rules apply to the connection using the parameters configured for **Probe Interval (seconds)** and **Failover Trigger Level (missed probes)** settings. If probing is enabled on dialup, the dialup connection is terminated and re-established when probing fails over the modem.
4. Select an option from the **Probe through** menu. Select **Ethernet Only** to probe the Ethernet WAN connection and failover to the modem when the connection is lost. Select **Modem Only** to probe a dial-up connection and have the modem redial when the dial-up connection is lost. Select **Modem and Ethernet** to enable both types of probing on the SP.
5. Enter the IP address for the probe target in the **Probe Target (IP Address)** field. The Probe IP address is a static IP address on the WAN. If this field is left blank, or 0.0.0.0 is entered as the address, the Probe Target is the WAN Gateway IP address.

✓ **Tip:** *The probe is a ping sent to the IP address and is used, along with the response, as a method of determining Internet connectivity.*

6. Select **ICMP Probing** or **TCP Probing** from the **Probe Type** options. If you select **TCP Probing**, enter the TCP port number in the **TCP port** field.
7. In the **Probe Interval (seconds)** field, enter the amount of time between probes to the **Probe Target**. The default value is **5** seconds. To deactivate the Probe Detection feature, enter *0* as the value. In this case, the WAN failover only occurs when loss of the physical WAN Ethernet connection occurs on the SonicWALL security appliance.
8. Enter the number of missed probes required for the WAN failover to occur in the **Failover Trigger Level (missed probes)** field.
9. Enter a value for the number of successful probes required to reactivate the primary connection in the **Successful Probes to Reactivate Primary** field. The default value is five (5). By requiring a number of successful probes before the SonicWALL security appliance returns to its primary connection, you can prevent the SonicWALL security appliance from returning to the primary connection before the primary connection becomes stable.
10. Click **Apply** for the settings to take effect on the SonicWALL security appliance.

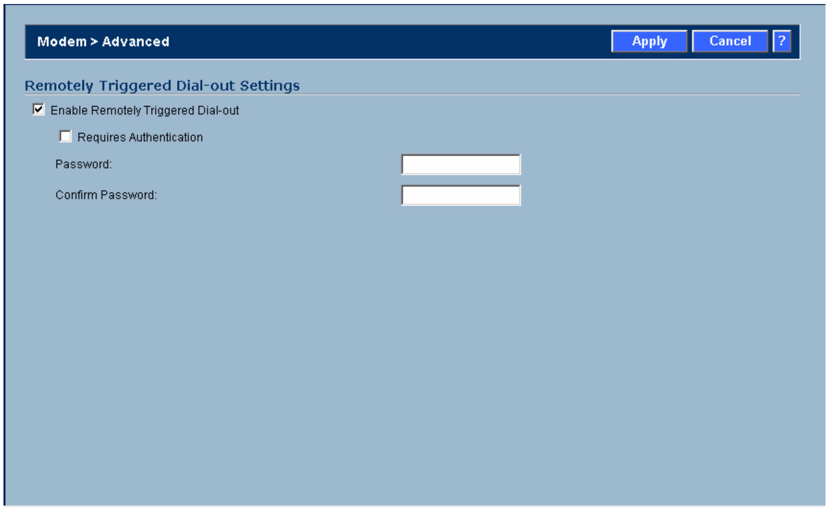
CHAPTER

20

Configuring Advanced Modem Settings

Modem > Advanced

The **Modem > Advanced** page allows you to configure the modem to be remotely triggered to dialout.



Remotely Triggered Dial-out Settings

☑ Enable Remotely Triggered Dial-out

☐ Requires Authentication

Password:

Confirm Password:

Check the **Enable Remotely Triggered Dial-out** box to enable this feature.

If you want user access to be authenticated by a password, check **Require Authentication**, and enter the password in the **Password** and **Confirm Password** fields.

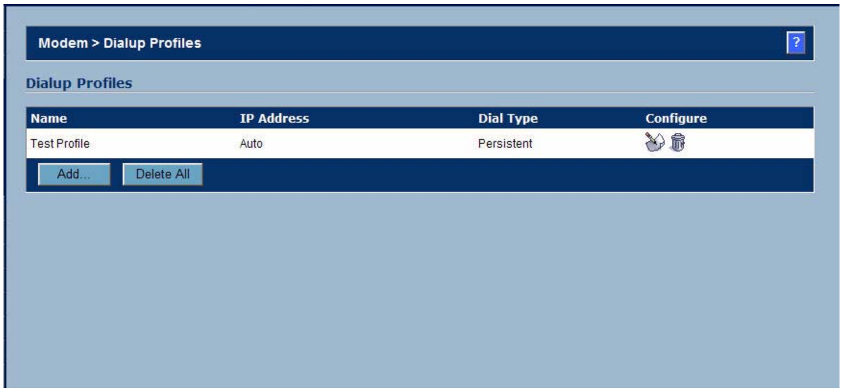
CHAPTER

21

Configuring Modem Dialup Properties

Modem > Dialup Profiles

The **Modem > Dialup Profiles** page allows you to configure modem profiles on the SonicWALL security appliance using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.



Modem > Dialup Profiles

Dialup Profiles

Name	IP Address	Dial Type	Configure
Test Profile	Auto	Persistent	✎ 🗑

✓ **Tip:** *The SonicWALL security appliance supports a maximum of 10 configuration profiles.*

Dial-Up Profiles

The current profile is displayed in the **Dialup Profiles** table, which displays the following dialup profile information:

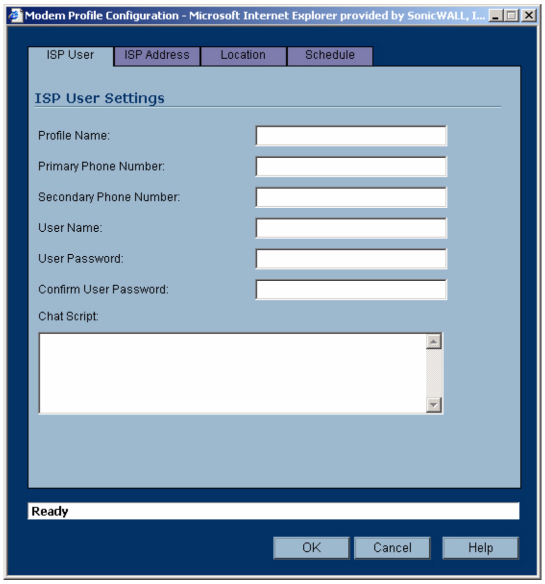
- **Name** - the name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - the IP address of the Internet connection.
- **Dial Type** - displays Persistent, Dial on Data, or Manual Dial, depending on what you selected in the **Modem Profile Configuration** window for the profile.
- **Configure** - clicking the **Notepad** icon allows you to edit the profile. Clicking on the **Trashcan** icon deletes the profile.

Configuring a Dialup Profile

In the **Modem > Dialup Profiles** page, click the **Add** button. The Modem Profile Configuration window is displayed for configuring a dialup profile.

Modem > Dialup Profiles > Modem Profile Configuration

The **Modem Profile Configuration** window allows you to configure your modem dial-up connections. Once you create your profiles, you can then configure specify which profiles to use for WAN failover or Internet access.


Modem Profile Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
ISP User
ISP Address
Location
Schedule
ISP User Settings
Profile Name:
Primary Phone Number:
Secondary Phone Number:
User Name:
User Password:
Confirm User Password:
Chat Script:
Ready
OK
Cancel
Help

Configuring a Dialup Profile

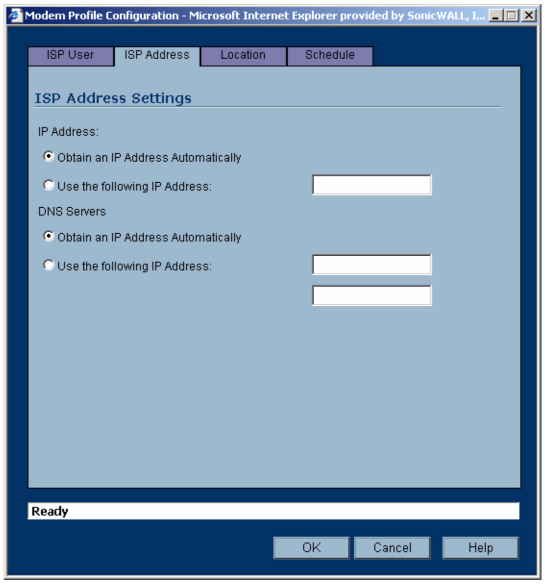
To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

1. In the **ISP User** page, enter a name for your dialup profile in the **Profile Name** field.
2. Enter the primary number used to dial your ISP in the **Primary Phone Number** field.

✓ **Tip:** *If a specific prefix is used to access an outside line, such as 9, &, or, , enter the number as part of the primary phone number.*

3. Enter the secondary number used to dial your ISP in the **Secondary Phone Number** field (optional).
4. Enter your dial-up ISP user name in the **User Name** field.
5. Enter the password provided by your dialup ISP in the **User Password** field.
6. Confirm your dialup ISP password in the **Confirm User Password** field.
7. If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information on Chat Scripts section for more information on using chat scripts.

8 Click the **ISP Address** tab.


Modem Profile Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
ISP User
ISP Address
Location
Schedule
OK
Cancel
Help

ISP Address Settings

IP Address:

● Obtain an IP Address Automatically

○ Use the following IP Address:

DNS Servers

● Obtain an IP Address Automatically

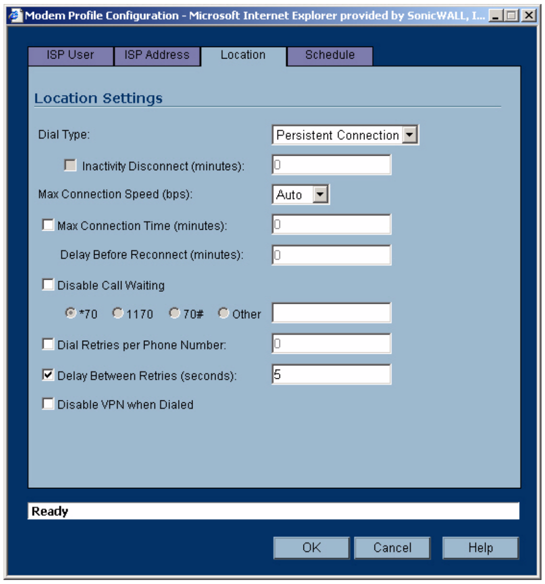
○ Use the following IP Address:

Ready

9 In the **ISP Address Setting** section, select **Obtain an IP Address Automatically** if you do not have a permanent dialup IP address from your ISP. If you have a permanent dialup IP address from your ISP, select **Use the following IP Address** and enter the IP address in the corresponding field.

10 If you obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**. If your ISP has a specific IP address for the DNS server(s), select **Use the following IP Address** and enter the IP address of the primary DNS server in the corresponding field. You can also add a secondary DNS server address in the field below.

11 Click on the **Location** tab. Use the settings in the page to configure modem dialup behavior.


Modem Profile Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
ISP User
ISP Address
Location
Schedule
OK
Cancel
Help

Location Settings

Dial Type: Persistent Connection

☐ Inactivity Disconnect (minutes): 0

Max Connection Speed (bps): Auto

☐ Max Connection Time (minutes): 0

Delay Before Reconnect (minutes): 0

☐ Disable Call Waiting

● *70 ○ 1170 ○ 70# ○ Other

☐ Dial Retries per Phone Number: 0

☑ Delay Between Retries (seconds): 5

☐ Disable VPN when Dialed

Ready

In the **Dial Type** menu select one of the following options:

- **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the Network > Settings page. If **Enable WAN Failover** is selected on the Modem>Failover page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

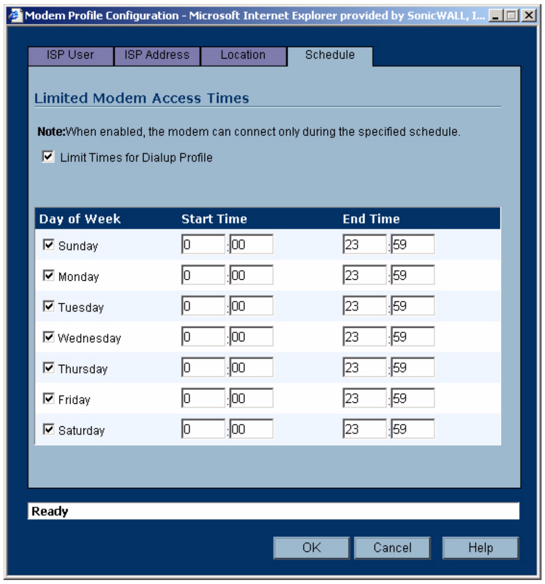
- **Dial on Data** - Using **Dial on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL security appliance internal applications such as AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the Modem > Failover page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Manual Dial** - Selecting **Manual Dial** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the Network>Settings page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

Alert: *If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.*

Alert: *If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking **Disconnect** on the **Configure** page.*

12. Enter the number of minutes a dial-up connection is allowed to be inactive in the **Inactivity Disconnect (minutes)** field.
13. Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the SonicWALL security appliance automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.
14. Select **Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.
15. If you select **Max Connection Time (minutes)**, enter the number of minutes to delay before redialling the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is 0 which means there is no delay before reconnecting to the ISP.
16. If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field.
17. If the phone number for your ISP is busy, you can configure the number of times that the SonicWALL security appliance modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.
18. Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.
19. Select **Disable VPN when Dialled** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.

20 Click on the **Schedule** tab.


Modem Profile Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
ISP User
ISP Address
Location
Schedule
OK
Cancel
Help

Limited Modem Access Times

Note: When enabled, the modem can connect only during the specified schedule.

☑ Limit Times for Dialup Profile

Day of Week	Start Time		End Time	
☑ Sunday	0	00	23	59
☑ Monday	0	00	23	59
☑ Tuesday	0	00	23	59
☑ Wednesday	0	00	23	59
☑ Thursday	0	00	23	59
☑ Friday	0	00	23	59
☑ Saturday	0	00	23	59

Ready

21 Select **Limit Times for Dialup Profile** to specify the scheduled times the modem is allowed to make connections.

22 Specify the days in the **Day of Week** column, and enter the time settings in the 24-hour format.

23 Click **OK** to add the dial-up profile to the SonicWALL security appliance. The Dialup Profile appears in the **Dialup Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to “chat” with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information. The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER**, **NO DIALTONE**, or **BUSY**are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreters waits for **OK** to be returned in response to the previous command, **ATV1**, before continuing the script. If OK is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If **OK** is received, the prefix and phone number of the selected dial-up account is dialled. The **\T** command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, **CONNECT** is the expected response from the remote modem. If the modems successfully connect, **CONNECT** is returned from the TELE3 SP modem.The **\D** adds a pause of one second to allow the server to start the PPP authentication. The **\C** command ends the chat script end without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, “chat script ppp Linux <ISP name>”.

A custom chat script can look like the following script:

```
ABORT `NO CARRIER'
ABORT `NO DIALTONE'
ABORT `BUSY'
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```

Tip: *The first character of username and password are ignored during PPP authentication.*

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after **CONNECT** which sends a carriage return command to the server. The chat interpreter then waits for **sername:** substring. When a response is returned, the current PPP account user name, substituting the **\L** command control string, is sent. Then, the chat interpreter waits for the substring assword:, and sends the password, substituting **\P** with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

PART 5

Wireless

CHAPTER 22

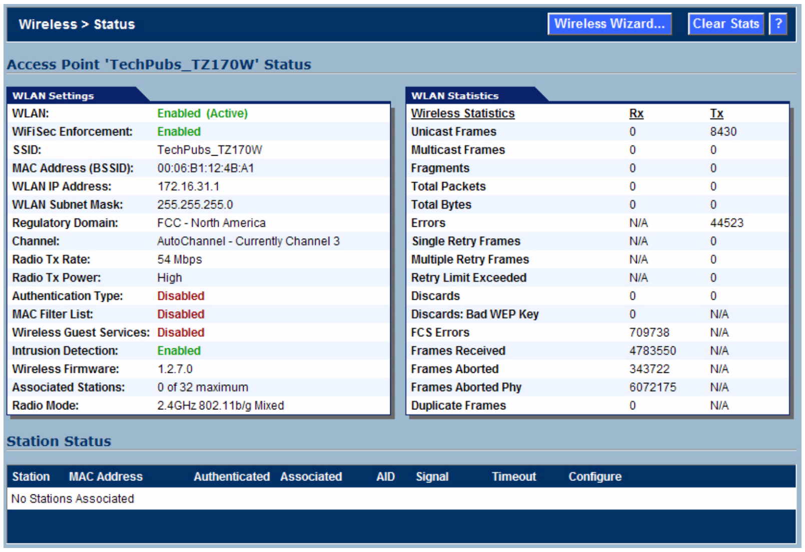
Setting Up the WLAN Using the Wireless Wizard and Monitoring Your WLAN

The SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 70 Wireless support two wireless protocols called IEEE 802.11b and 802.11g, commonly known as Wi-Fi, and sends data via radio transmissions. The TZ 150 Wireless/TZ 170 Wireless combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless offer the flexibility of wireless without compromising network security.

Typically, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an "always-on" connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to "eavesdropping" by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Access to Wireless Guest Services (WGS) and MAC Filter Lists are managed by the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. It is also at this layer that the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless has the capability of enforcing WiFiSec, an IPSec-based VPN overlay for wireless networking. As wireless network traffic successfully passes through these layers, it is then passed to the VPN-NAT-Stateful firewall layer where WiFiSec termination, address translation, and access rules are applied. If all of the security criteria is met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- VPN tunnel



Access Point 'TechPubs_TZ170W' Status

WLAN Settings

WLAN:	Enabled (Active)
WiFiSec Enforcement:	Enabled
SSID:	TechPubs_TZ170W
MAC Address (BSSID):	00:06:B1:12:4B:A1
WLAN IP Address:	172.16.31.1
WLAN Subnet Mask:	255.255.255.0
Regulatory Domain:	FCC - North America
Channel:	AutoChannel - Currently Channel 3
Radio Tx Rate:	54 Mbps
Radio Tx Power:	High
Authentication Type:	Disabled
MAC Filter List:	Disabled
Wireless Guest Services:	Disabled
Intrusion Detection:	Enabled
Wireless Firmware:	1.2.7.0
Associated Stations:	0 of 32 maximum
Radio Mode:	2.4GHz 802.11b/g Mixed

WLAN Statistics

Wireless Statistics	Rx	Tx
Unicast Frames	0	8430
Multicast Frames	0	0
Fragments	0	0
Total Packets	0	0
Total Bytes	0	0
Errors	N/A	44523
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	0
Discards	0	0
Discards: Bad WEP Key	0	N/A
FCS Errors	709738	N/A
Frames Received	4783550	N/A
Frames Aborted	343722	N/A
Frames Aborted Phy	6072175	N/A
Duplicate Frames	0	N/A

Station Status

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
No Stations Associated							

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is a firewall and has NAT capabilities which provides security, and you can use WiFiSec to secure data transmissions.

Optimal Wireless Performance Recommendations

- Place the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless and the receiving points such as PCs or laptops.
- Try to place theTZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless near walls, fireplaces, or other large solid objects. Placing the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is installed near these types of materials.
- Installing the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless.

Adjusting the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless Antennas

The antennas on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Guest Services (WGS)

With your TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, you can provide wireless guest services to wireless-equipped users who are not part of your corporate network, for example, a consultant or a sales person. You can offer authenticated wireless users access to the Internet through your TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless while preventing access to your corporate LAN, or allowing them access to specific resources on the LAN and unencrypted access to the Internet.

When WGS is active, wireless clients can authenticate and associate with the Access Layer of the SonicWALL. When a Web browser is launched, the wireless user is prompted to provide a user name and password to gain access to WGS. The browser is redirected to the HTTP (unencrypted) management address of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, but the user name and password is not transmitted. Instead, a secure hash is transmitted rendering the information useless to anyone “eavesdropping” on the network. After authentication, users are tracked and controlled by the client MAC address as well as Account and Session lifetimes.

In order to take advantage of Wireless Guest Services, you must provide a guest with a user name and password which they use to authenticate themselves using HTTP and a Web browser, creating a secure HTTP session.

Wireless Node Count Enforcement

Users on the WLAN are not counted towards the node enforcement on the SonicWALL. Only users on the LAN are counted towards the node limit.

MAC Filter List

The SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless networking protocol provides native MAC address filtering capabilities. When MAC address filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

The TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless uses WGS to overcome this limitation by moving MAC address filtering to the Secure Wireless Gateway layer. This allows wireless users to authenticate and associate with the Access Point layer of the SonicWALL, and be redirected to the WGS by the Secure Wireless Gateway where the user authenticates and obtains WLAN to WAN access.

Easy WGS MAC Filtering is an extension of WGS that simplifies the administrative burden of manually adding MAC addresses to the MAC Filter List. Users can add themselves to the MAC Filter List by providing a user name and password assigned to them by the SonicWALL administrator. WGS must be enabled on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless before Easy MAC Filter List can be implemented.

WiFiSec Enforcement

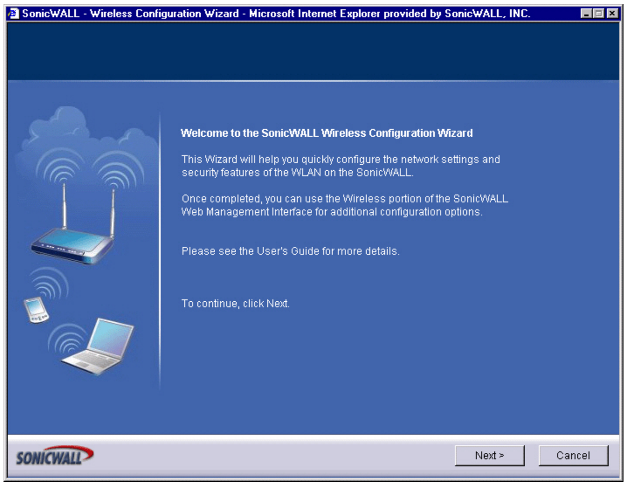
Enabling **WiFiSec Enforcement** on the SonicWALL enforces the use of IPSec-based VPN for access from the WLAN to the WAN or LAN, and provides access from the WLAN to the WAN independent of WGS. Access from one wireless client to another is configured on the **Wireless>Advanced** page where you can disable or enable access between wireless clients.

WiFiSec uses the easy provisioning capabilities of the SonicWALL Global VPN client making it easy for experienced and inexperienced administrators to implement on the network. The level of interaction between the Global VPN Client and the user depends on the WiFiSec options selected by the administrator. WiFiSec IPSec terminates on the WLAN/LAN port, and is configured using the Group VPN Security Policy including noneditable parameters specifically for wireless access.

Using the Wireless Wizard

You can use the Wireless Wizard to quickly and easily set up your wireless network. Log into the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, and click **Wireless** on the menu bar. Click **Wireless Wizard** to launch the wizard and begin the configuration process. Or click **Wizards**, and select **Wireless Wizard**.

Welcome to the SonicWALL Wireless Configuration Wizard


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Wireless Configuration Wizard

This Wizard will help you quickly configure the network settings and security features of the WLAN on the SonicWALL.

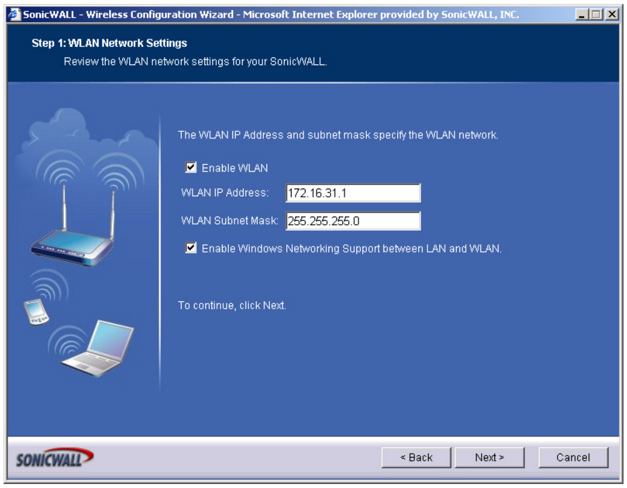
Once completed, you can use the Wireless portion of the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.

1 When the Wireless Wizard launches, the **Welcome** page is displayed. Click **Next** to continue configuration.

WLAN Network Settings


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 1: WLAN Network Settings

Review the WLAN network settings for your SonicWALL.

The WLAN IP Address and subnet mask specify the WLAN network.

☑ Enable WLAN

WLAN IP Address: 172.16.31.1

WLAN Subnet Mask: 255.255.255.0

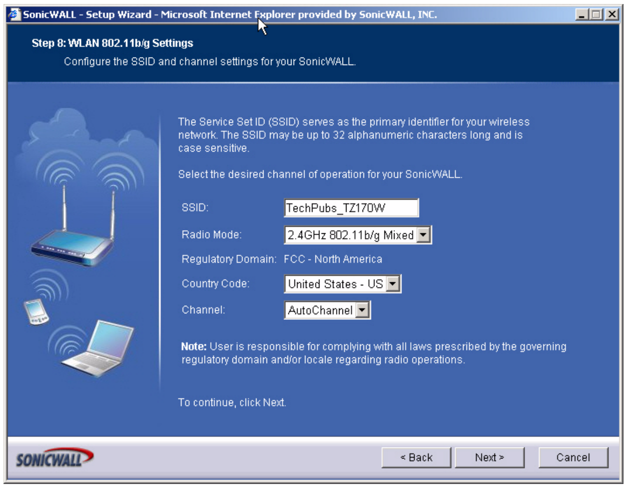
☑ Enable Windows Networking Support between LAN and WLAN.

To continue, click Next.

2 Select the **Enable WLAN** check box to activate the wireless feature of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. Use the default IP address for the WLAN or choose a different private IP address. The default value works for most networks. The **Enable Windows Networking Support between LAN and WLAN** to allow wireless clients to access your Windows network resources, such as shared folders and printers. Click **Next** to continue.

▲ **Alert:** *You cannot use the same private IP address range as the LAN port of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless.*

WLAN 802.11b Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 8: WLAN 802.11b/g Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the desired channel of operation for your SonicWALL.

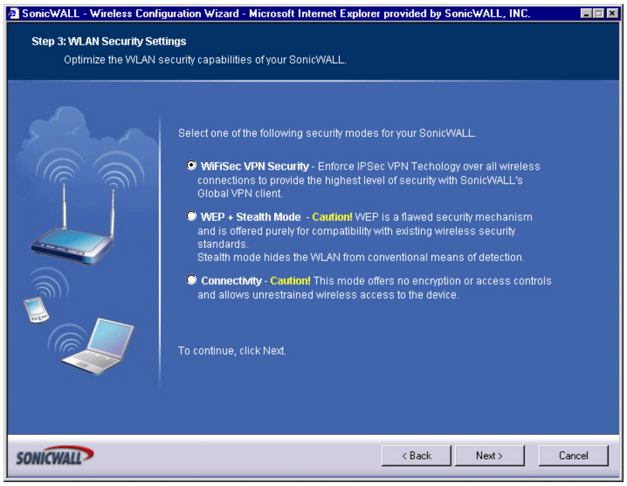
SSID: TechPubs_TZ170W
Radio Mode: 2.4GHz 802.11b/g Mixed
Regulatory Domain: FCC - North America
Country Code: United States - US
Channel: AutoChannel

Note: User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

To continue, click Next.

3 Type a unique identifier for the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless in the SSID field. It can be up to 32 alphanumeric characters in length and is case-sensitive. The default value is **sonicwall**.

WLAN Security Settings


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: WLAN Security Settings

Optimize the WLAN security capabilities of your SonicWALL.

Select one of the following security modes for your SonicWALL.

● **WiFiSec VPN Security** - Enforce IPSec VPN Techology over all wireless connections to provide the highest level of security with SonicWALL's Global VPN client.

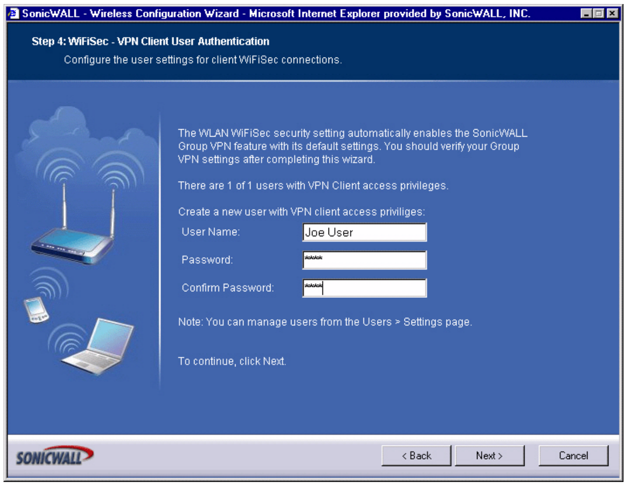
○ **WEP + Stealth Mode** - **Caution!** WEP is a flawed security mechanism and is offered purely for compatibility with existing wireless security standards.
Stealth mode hides the WLAN from conventional means of detection.

○ **Connectivity** - **Caution!** This mode offers no encryption or access controls and allows unrestrained wireless access to the device.

To continue, click Next.

4 Choose the desired security setting for the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. **WiFiSec** is the most secure and enforces IPSec over the wireless network. If you have an existing wireless network and want to use the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, select **WEP + Stealth Mode**.

WiFiSec - VPN Client User Authentication


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: WiFiSec - VPN Client User Authentication

Configure the user settings for client WiFiSec connections.

The WLAN WiFiSec security setting automatically enables the SonicWALL Group VPN feature with its default settings. You should verify your Group VPN settings after completing this wizard.

There are 1 of 1 users with VPN Client access privileges.

Create a new user with VPN client access priviliges:

User Name: Joe User

Password: ****

Confirm Password: ****

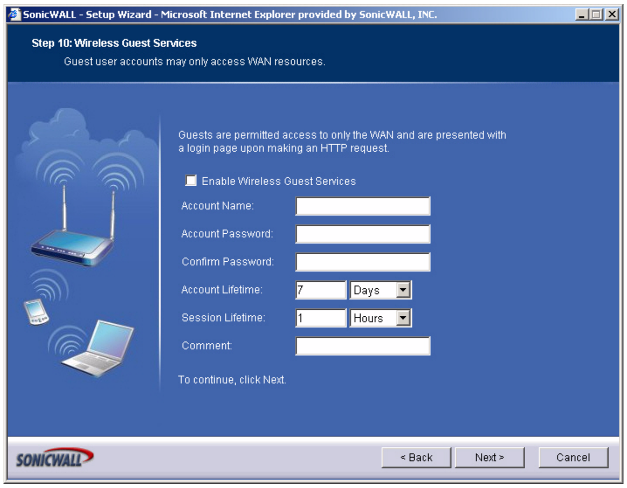
Note: You can manage users from the Users > Settings page.

To continue, click Next.

5 Create a new user with VPN Client privileges by typing a user name and password in the **User Name** and **Password** fields.

Alert: *Selecting WiFiSec automatically enables the SonicWALL Group VPN feature and its default settings. Verify your Group VPN settings after configuring your wireless connection.*

Wireless Guest Services


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 10: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access to only the WAN and are presented with a login page upon making an HTTP request.

☐ Enable Wireless Guest Services

Account Name:

Account Password:

Confirm Password:

Account Lifetime: 7 Days

Session Lifetime: 1 Hours

Comment:

To continue, click Next.

6 The **Enable Wireless Guest Services** check box is selected by default. You can create guest wireless accounts to grant access to the WAN only.

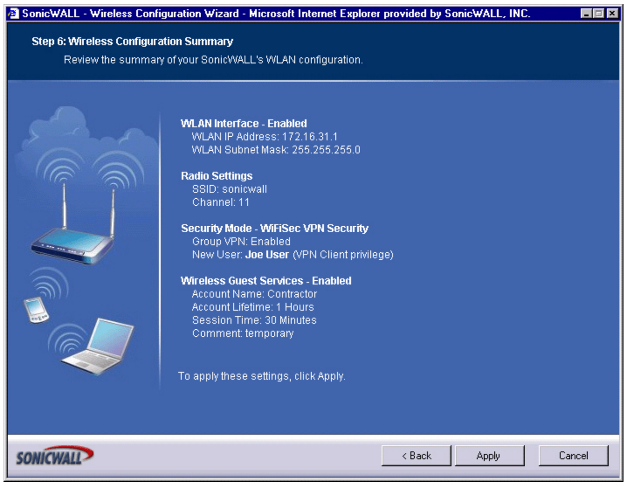
If you enable Wireless Guest Services, type a name for the account in the **Account Name** field, and a password in the **Account Password** field.

The **Account Lifetime** is set to one hour by default, but you can configure **Minutes**, **Hours**, or **Days** to determine how long the guest account is active.

Type the value in the **Session Timeout** field. Select **Minutes**, **Hours**, or **Days**.

Any comments about the connection can be typed in the **Comment** field.

Wireless Configuration Summary


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Apply
Cancel

Step 6: Wireless Configuration Summary

Review the summary of your SonicWALL's WLAN configuration.

WLAN Interface - Enabled
WLAN IP Address: 172.16.31.1
WLAN Subnet Mask: 255.255.255.0

Radio Settings
SSID: sonicwall
Channel: 11

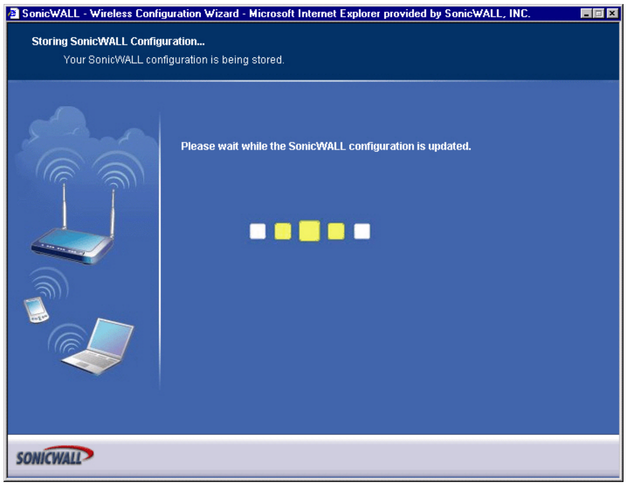
Security Mode - WiFiSec VPN Security
Group VPN: Enabled
New User: **Joe User** (VPN Client privilege)

Wireless Guest Services - Enabled
Account Name: Contractor
Account Lifetime: 1 Hours
Session Time: 30 Minutes
Comment: temporary

To apply these settings, click Apply.

7 Review your wireless settings for accuracy. If you want to make changes, click **Back** until the settings are displayed. Then click **Next** until you reach the **Summary** page.

Updating the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

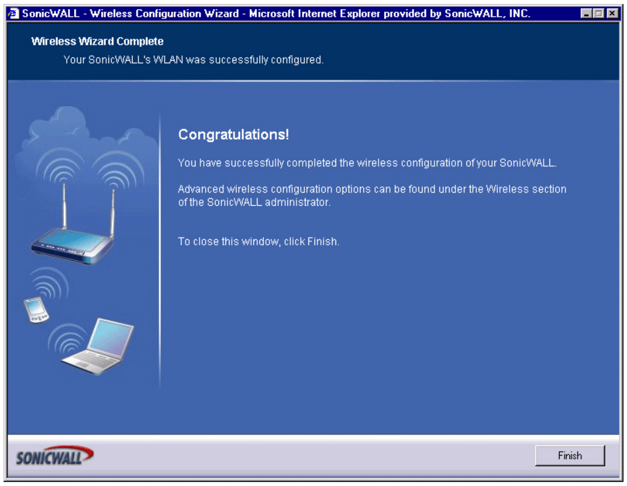
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

8 The TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is now updating the wireless configuration with your settings.

Congratulations


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Finish

Wireless Wizard Complete

Your SonicWALL's WLAN was successfully configured.

Congratulations!

You have successfully completed the wireless configuration of your SonicWALL.

Advanced wireless configuration options can be found under the Wireless section of the SonicWALL administrator.

To close this window, click Finish.

9 Congratulations! You have successfully completed configuration of your wireless settings. Click **Finish** to exit the Wizard.

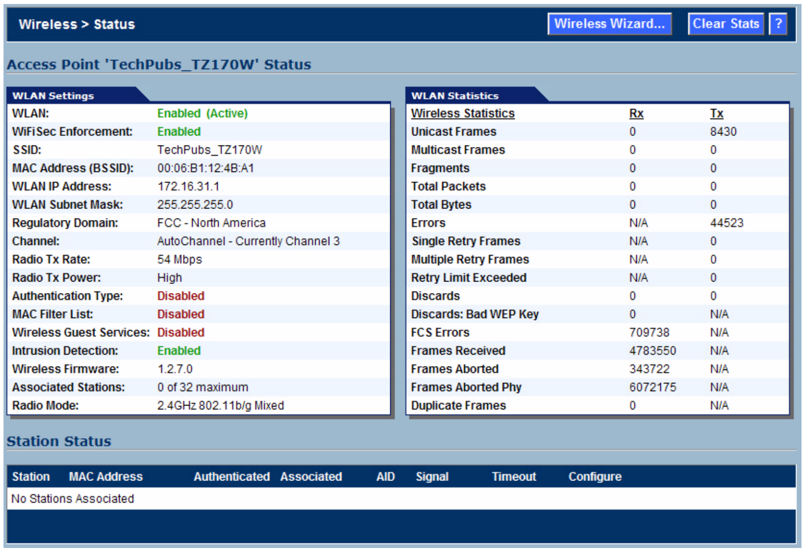
Configuring Additional Wireless Features

The SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless has the following features available:

- **WiFiSec Enforcement** - an IPSec-based VPN overlay for wireless networking
- **WEP Encryption** - configure Wired Equivalent Privacy (WEP) Encryption
- **Beaconing and SSID Controls** - manage transmission of the wireless signal.
- **Wireless Client Communications** - configure wireless client settings.
- **Advanced Radio Settings** - fine-tune wireless broadcasting.
- **MAC Filtering** - use MAC addresses for allowing access or blocking access.

Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, and **Station Status**.



Access Point 'TechPubs_TZ170W' Status

WLAN Settings

WLAN:	Enabled (Active)
WiFiSec Enforcement:	Enabled
SSID:	TechPubs_TZ170W
MAC Address (BSSID):	00:06:B1:12:4B:A1
WLAN IP Address:	172.16.31.1
WLAN Subnet Mask:	255.255.255.0
Regulatory Domain:	FCC - North America
Channel:	AutoChannel - Currently Channel 3
Radio Tx Rate:	54 Mbps
Radio Tx Power:	High
Authentication Type:	Disabled
MAC Filter List:	Disabled
Wireless Guest Services:	Disabled
Intrusion Detection:	Enabled
Wireless Firmware:	1.2.7.0
Associated Stations:	0 of 32 maximum
Radio Mode:	2.4GHz 802.11b/g Mixed

WLAN Statistics

Wireless Statistics	Rx	Tx
Unicast Frames	0	8430
Multicast Frames	0	0
Fragments	0	0
Total Packets	0	0
Total Bytes	0	0
Errors	N/A	44523
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	0
Discards	0	0
Discards: Bad WEP Key	0	N/A
FCS Errors	709738	N/A
Frames Received	4783550	N/A
Frames Aborted	343722	N/A
Frames Aborted Phy	6072175	N/A
Duplicate Frames	0	N/A

Station Status

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
No Stations Associated							

WLAN Settings

In addition to providing different status views for **Access Point** and **Wireless Bridge** modes, two new functions have been added to the **Wireless > Status** page:

Hyperlinked WLAN Settings - All configurable WLAN settings are now hyperlinked to their respective pages for configuration. (Present in both Access Point and Wireless Bridge modes). Enabled features are displayed in green, and disabled features are displayed in red.

Automated Station Blocking - Previously, the **Station Status** view allowed for stations to be added to the MAC allow list, or disassociated from the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. The disassociated station, however, could easily re-associate unless other prohibitive actions were taken. This functionality has been enhanced by adding the **Block** icon. Clicking this icon disassociates the station and adds the station to the MAC block list.To begin configuring advanced features on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, log into the management interface, and click **Wireless**. The **Status** page is displayed and contains information relating to the WLAN connection.

Access Point Status

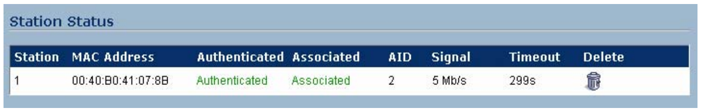
WLAN Settings	Value
WLAN:	Enabled or Disabled
WiFiSec:	Enabled or Disabled
SSID:	Network Identification Information
MAC Address:	Serial Number of the TZ 150 Wireless/TZ 170 Wireless
WLAN IP Address:	IP address of the WLAN port
WLAN Subnet Mask:	Subnet information
Regulatory Domain	**FCC - North America** for domestic appliances **ETSI - Europe** for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	the current power level of the radio signal transmission
Authentication Type	the type of WEP or PSK authentication or Disabled
MAC Filter List	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Wireless Firmware:	Firmware versions on the radio card
Associated Stations:	Number of clients associated with the TZ 150 Wireless/TZ 170 Wireless
Radio Mode	Radio Frequency and 802.11 mode: 2.4GHz 802.11b/g Mixed, 2.4GHz 802.11g Only, or 2.4GHz 802.11b Only

WLAN Statistics

802.11b Frame Statistics	Rx/TX
Unicast Frames	Number of frames received and transmitted
Multicast Frames	Total number of frames received and transmitted as broadcast or multicast. Typically a lower number than Unicast frames.
Fragments	Total number of fragmented frames received and sent. This is a general indication of activity at this wireless device.
Total Packets	Total number of packets received and transmitted
Total Bytes	Total number of bytes received and transmitted
Errors	Total number of receive and transmit errors
Single Retry Frames	Number of messages retransmitted a single time being acknowledged by the receiving device. Retransmission is normal for 802.11b to quickly recover from lost messages.
Multiple Retry Frames	Number of messages retransmitted multiple times before acknowledgement by the receiving device. A relatively high value can indicate interference or a heavy wireless data load.
Retry Limit Exceeded	Number of messages undelivered after the maximum number of transmissions. Along with Discards, it can indicate a wireless network under heavy interference or excessive load of wireless data traffic.
Discards	Number of messages untransmitted due to congestion. Normally, the messages are temporarily stored in an internal buffer until transmitted. When the buffer is full, frames are discarded until the buffer is cleared. When the number is high, it may indicate a wireless network with a heavy load of traffic.
Discards: Bad WEP Key	Number of times a received message was discarded because it could not be decrypted. This could indicate mismatched keys or one device does not support encryption or does not have encryption enabled.
FCS Errors	Number of received frames or frame parts containing an erroneous checksum requiring deletion. Messages are recovered using ACK and retransmitted by the sending device.
Frames Received	Total number of data frames received.
Frames Aborted	Total number of frames dropped.
Frames Aborted Phy	
Duplicate Frames	Number of duplicate frames received.

Station Status

The **Station Status** table displays information about wireless connections associated with the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless.



Station Status

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Delete
1	00:40:B0:41:07:8B	Authenticated	Associated	2	5 Mb/s	299s	🗑

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated -** status of 802.11b authentication

- **Associated** - status of 802.11b association
- **AID** - assigned by the SonicWALL
- **Signal**- frequency in Mbps
- **Timeout** - number of seconds left on the session
- **Delete** - delete the entry from the MAC Filter List.

CHAPTER

23

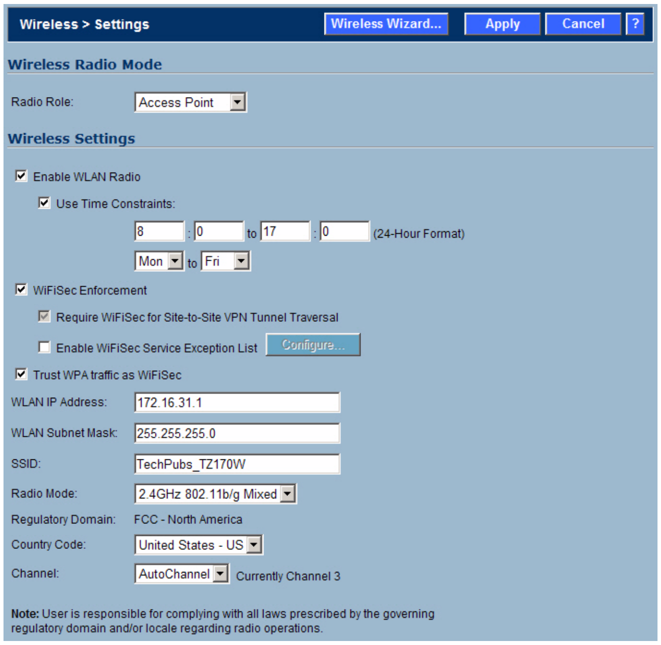
Configuring Wireless Settings

Wireless > Settings

The **Wireless > Settings** page allows you to configure your wireless settings.

Note: *The SonicWALL TZ 50 Wireless and TZ 150 Wireless does not support wireless bridging mode.*

On the **Wireless>Settings** page, you can enable or disable the WLAN port by selecting or clearing the **Enable WLAN** checkbox.



Wireless Radio Mode

Radio Role: Access Point

Wireless Settings

☑ Enable WLAN Radio
  ☑ Use Time Constraints:
  8 : 0 to 17 : 0 (24-Hour Format)
  Mon to Fri
☑ WiFiSec Enforcement
  ☑ Require WiFiSec for Site-to-Site VPN Tunnel Traversal
  ☐ Enable WiFiSec Service Exception List
☑ Trust WPA traffic as WiFiSec

WLAN IP Address: 172.16.31.1
WLAN Subnet Mask: 255.255.255.0
SSID: TechPubs_TZ170W
Radio Mode: 2.4GHz 802.11b/g Mixed
Regulatory Domain: FCC - North America
Country Code: United States - US
Channel: AutoChannel Currently Channel 3

Note: User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

Wireless Radio Mode

Select either **Access Point** to configure the SonicWALL as the default gateway on your network or select **Bridge Mode** from the **Radio Role** menu to configure the SonicWALL to act as an intermediary wireless device.

Note: *WPA support is only available in Access Point Mode. WPA support is not available in Bridge Mode.*

Wireless Settings

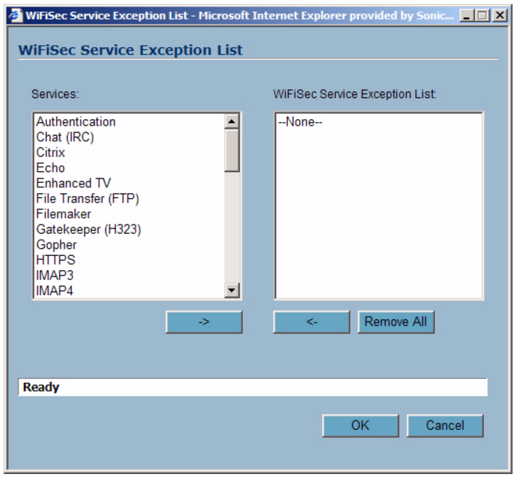
Enable WLAN Radio: Enable the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless radio for wireless connections.

Use Time Constraints: Only enable the radio during the times you specify.

WiFiSec Enforcement: Select this setting to provide IPSec-based VPN on a WLAN. If selected, wireless clients must download a copy of the Global VPN Client software to install on their computer. You must also configure and enable the Group VPN Security Association. When the **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** setting is enabled, any wireless traffic destined for a remote network with a VPN tunnel is secured by WiFiSec. The **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** checkbox is enabled by default.

When the **Enable WiFiSec Service Exception List** setting is enabled, serrvices you specify in the WiFiSec exception list do not require WiFiSec to connect. To configure the WiFiSec exception list:

1 Click **Configure** next to **Enable WiFiSec Service Exception List**.


WiFiSec Service Exception List - Microsoft Internet Explorer provided by Sonic...
WiFiSec Service Exception List
Services:
WiFiSec Service Exception List:
Authentication
Chat (IRC)
Citrix
Echo
Enhanced TV
File Transfer (FTP)
Filemaker
Gatekeeper (H323)
Gopher
HTTPS
IMAP3
IMAP4
--None--
->
<-
Remove All
Ready
OK
Cancel

2 In the **WiFiSec Service Exception List** window, select the services you want to exclude in the **Services** column.

3 Click the -> button to move the services into the **WiFiSec Service Exception List** column.

4 When you have the list elements you want, click **OK**.

WLAN IP Address/WLAN Subnet Mask: You can configure a different IP address for the WLAN by typing another private IP address in the **WLAN IP Address** field. Type the subnet in the **Subnet Mask** field. Click **Apply** for the changes to take effect on the SonicWALL.

SSID: The default value, **sonicwall**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

Radio Mode: Select your preferred radio mode from the **Radio Mode** menu. The TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless supports the following modes:

- **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.

- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

Regulatory Domain: Specifies the regulatory domain whose radio broadcasting rules the security appliance must obey. This field is determined by the ROM code.

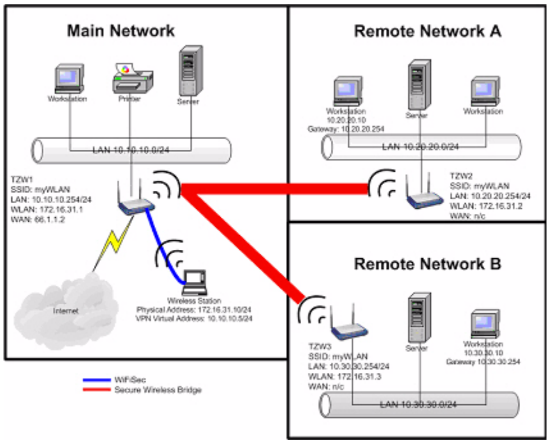
Country Code: Specifies the country within the regulatory domain where the SonicWALL TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is deployed.

Channel: Select the channel for transmitting the wireless signal from the **Channel** menu. An **AutoChannel** setting allows the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. AutoChannel is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.

Secure Wireless Bridging (TZ 170 Only)

The SonicWALL TZ 50 Wireless and TZ 150 Wireless does not support wireless bridging mode.

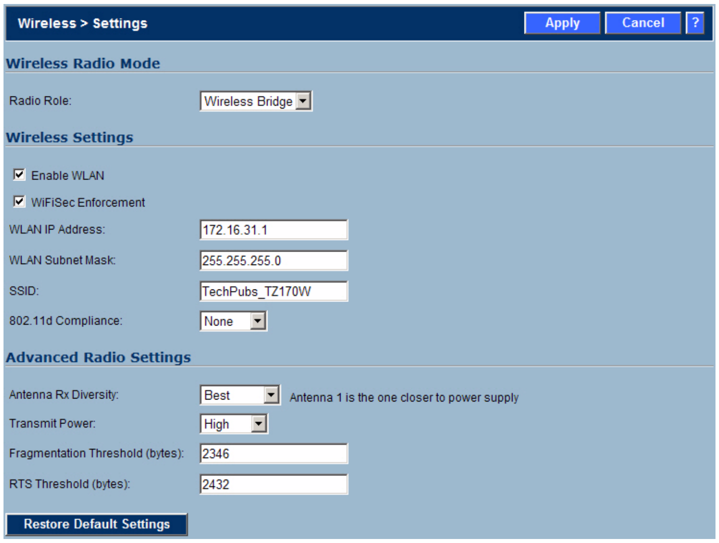
Wireless Bridging is a feature that allows two or more physically separated networks to be joined over a wireless connection. The TZ 170 Wireless provides this capability by shifting the radio mode at remote networks from **Access Point** mode to **Wireless Bridge** mode. Operating in Wireless Bridge mode, the TZ 170 Wireless connects to another TZ 170 Wireless acting as an access point, and allows communications between the connected networks via the wireless bridge.


Main Network
Workstation
Printer
Server
LAN 10.10.10.0/24
TZW1
SSID: myWLAN
LAN: 10.10.10.254/24
WLAN: 172.16.31.1
WAN: 66.1.1.2
Internet
Wireless Station
Physical Address: 172.16.31.10/24
VPN Virtual Address: 10.10.10.5/24
WiFiSec
Secure Wireless Bridge
Remote Network A
Workstation
10.20.20.10
Gateway: 10.20.20.254
Server
Workstation
LAN 10.20.20.0/24
TZW2
SSID: myWLAN
LAN: 10.20.20.254/24
WLAN: 172.16.31.2
WAN: n/c
Remote Network B
TZW3
SSID: myWLAN
LAN: 10.30.30.254/24
WLAN: 172.16.31.3
WAN: n/c
Server
Workstation
10.30.30.10
Gateway 10.30.30.254
LAN 10.30.30.0/24

Secure Wireless Bridging employs a WiFiSec VPN policy, providing security to all communications between the wireless networks. Previous bridging solutions offered no encryption, or at best, WEP encryption.

Configuring a Secure Wireless Bridge

When switching from **Access Point** mode to **Wireless Bridge** mode, all clients are disconnected, and the navigation panel on the left changes to reflect the new mode of operation.



Wireless Radio Mode

Radio Role: Wireless Bridge

Wireless Settings

☑ Enable WLAN

☑ WiFiSec Enforcement

WLAN IP Address: 172.16.31.1

WLAN Subnet Mask: 255.255.255.0

SSID: TechPubs_TZ170W

802.11d Compliance: None

Advanced Radio Settings

Antenna Rx Diversity: Best Antenna 1 is the one closer to power supply

Transmit Power: High

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2432

To configure a secure wireless bridge, follow these steps:

1. Click **Wireless**, then **Advanced**.
2. In the **Wireless Radio Mode** section, select **Wireless Bridge** from the **Radio Role** menu. The TZ 170 Wireless updates the interface.
3. Click **Status**. Any available access point is displayed at the bottom of the **Status** page. Click **Connect** to establish a wireless bridge to another TZ 170 Wireless.
4. Click **Settings**. Configure the WLAN settings for the wireless connection as follows:
    a. Configure the SSID on all TZ 170 Wireless to the SSID of the Access Point.
    b. Configure the WLAN for all TZ 170 Wireless must be on the same subnet.
    c. LAN IP address for all TZ 170 Wireless must be on different subnets.

For example, in the previous network diagram, the TZ 170 Wireless are configured as follows:

- SSID on all three TZ 170 Wireless are set to “myWLAN”.
- WLAN addressing for all the TZ 170 Wireless's connected via Wireless Bridge must place the WLAN interfaces on the same subnet: 172.16.31.1 for TZ 170 Wireless1, 172.16.31.2 for TZ 170 Wireless2, and 172.16.31.3 for TZ 170 Wireless3.
- TZ 170 Wireless4 must have a different subnet on the WLAN, such as 172.16.32.X/24.
- LAN addressing for all TZ 170 Wireless connected via Wireless Bridge must place the LAN interfaces on different subnets: 10.10.10.x/24 for TZ 170 Wireless1, 10.20.20.x/24 for TZ 170 Wireless2, and 10.30.30.x/24 for TZ 150 Wireless/TZ 170 Wireless3.
- LAN addressing for TZ 170 Wireless4 must be the same as TZ 170 Wireless3.
- To facilitate Virtual Adapter addressing, the TZ 170 Wireless4 can be set to forward DHCP requests to TZ 170 Wireless3.
- When a TZ 170 Wireless is in Wireless Bridge mode, the channel cannot be configured. TZ 170 Wireless2 and TZ 170 Wireless3 operate on the channel of the connecting Access Point TZ 170 Wireless. For example, TZ 170 Wireless1 is on channel 1.
- A Bridge Mode TZ 170 Wireless cannot simultaneously support wireless client connections. Access Point services at Remote Site B are provided by a second TZ 170 Wireless (4). The channel of operation is set 5 apart from the channel inherited by the TZ 170 Wireless3. For example, Access Point TZ 170 Wireless1 is set to channel 1, then Bridge Mode TZ 170 Wireless3 inherits channel 1. Access Point TZ 170 Wireless4 should be set to channel 6.

Network Settings for the Example Network

Device	Mode	SSID	Channel	LAN IP Address	WLAN IP Address
TZ 170 Wireless1	Access Point	myWLAN	1	10.10.10.254/24	172.16.31.1/24
TZ 170 Wireless2	Wireless Bridge	myWLAN	1 (auto)	10.20.20.254/24	172.16.31.2/24
TZ 170 Wireless3	Wireless Bridge	myWLAN	1 (auto)	10.30.30.254/24	172.16.31.3/24
TZ 170 Wireless4	Access Point	otherWLAN	6	10.30.30.253/24	172.16.31.1/24

Wireless Bridging (without WiFiSec)

To provide compatibility with other non-WiFiSec wireless access points, the TZ 170 Wireless supports a non-secure form of wireless bridging, but insecure wireless communications should only be employed when data is non-sensitive. By default, **WiFiSec Enforcement** is enabled on **Wireless Settings** for **Wireless Bridge** Mode. To connect to a non-WiFiSec access point, this checkbox must be disabled. Since VPN tunnels are not established in non-secure Wireless Bridging deployments, traffic routes must be clearly defined for both the Access Point and the Bridge Mode sites:

- The default route on the Bridge Mode TZ 170 Wireless must from the WLAN interface to the WLAN interface of the connecting Access Point TZ 170 Wireless.
  - Referring to the example above, the default route on TZ 170 Wireless2 and TZ 170 Wireless3 is set via their WLAN interfaces to 172.16.31.1.
- Static routes must be entered on the Access Point TZ 170 Wireless to route back to the LAN subnets of the Bridge Mode TZ 170 Wireless.
  - Referring to the example network, TZ 170 Wireless1 must have static routes to 10.20.20.x/24 via 172.16.31.2 and to 10.30.30.x/24 via 172.16.31.3

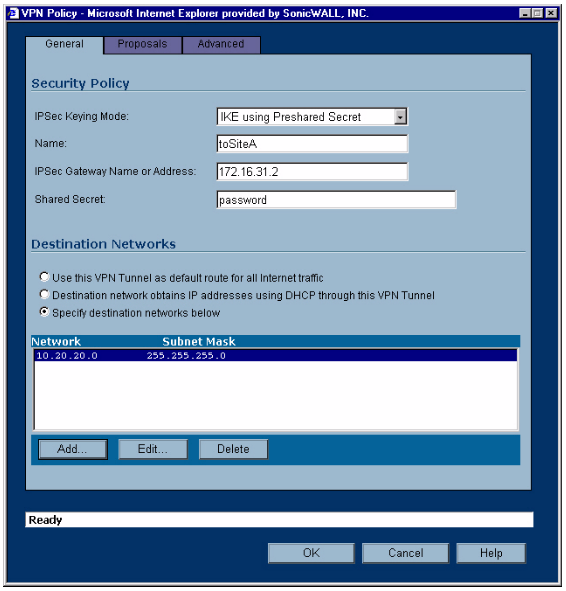
Configuring VPN Policies for the Access Point and Wireless Bridge

Access Point

After Wireless Settings are defined, the WiFiSec connections (VPN Policies) must be configured. The VPN Policies are defined as would any other site-to-site VPN policy, typically with the following in mind:

- The Access Point TZ 150 Wireless/TZ 170 Wireless must specify the destination networks of the remote sites.
- The Access Point TZ 150 Wireless/TZ 170 Wireless must specify its LAN management IP address as the **Default LAN Gateway** under the **Advanced** tab.
- The Wireless Bridge Mode TZ 170 Wireless must be configured to use the tunnel as the default route for all internet traffic.

Referring to our example network, the Access Point TZ 170 Wireless has the following two VPN Policies defined:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Add...
Edit...
Delete
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: toSiteA

IPSec Gateway Name or Address: 172.16.31.2

Shared Secret: password

Destination Networks

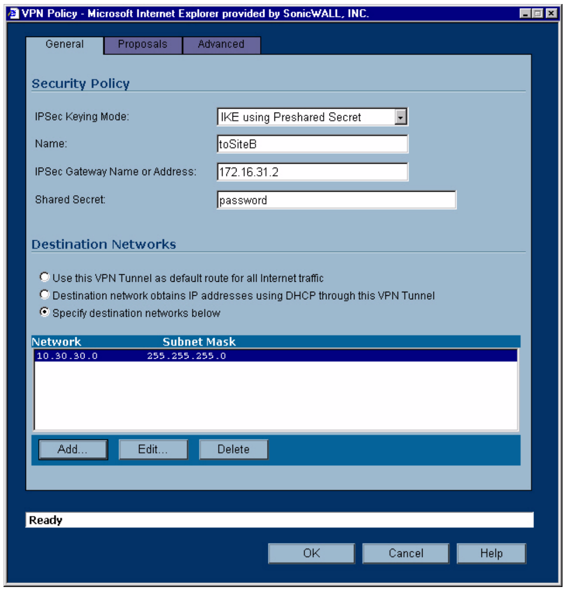
○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Specify destination networks below

Network	Subnet Mask
10.20.20.0	255.255.255.0

Ready


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Add...
Edit...
Delete
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: toSiteB

IPSec Gateway Name or Address: 172.16.31.2

Shared Secret: password

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Specify destination networks below

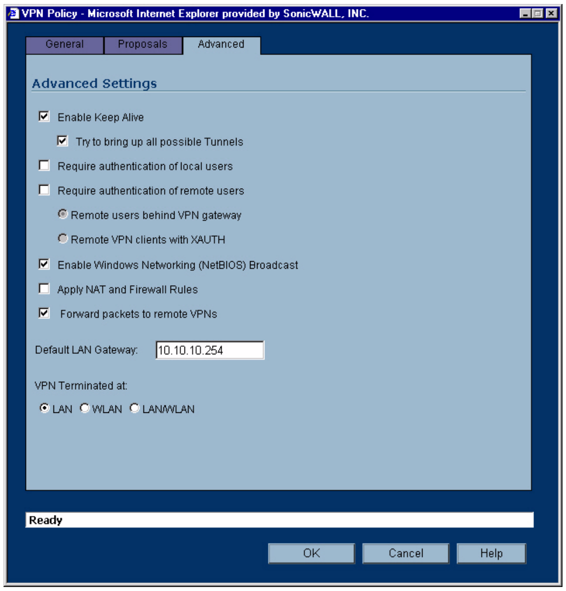
Network	Subnet Mask
10.30.30.0	255.255.255.0

Ready

Advanced Configuration for both VPN Policies

1. Click **Advanced**.
2. Select **Enable Keep Alive** and **Try to bring up all possible tunnels**.
3. Select **Enable Windows Networking (NetBIOS) Broadcast**.
4. Select **Forward Packets to remote VPNs**.
5. Enter the LAN IP address of the Access Point in the **Default LAN Gateway** field.
6. Select **LAN** for **VPN Terminated at**.

7 Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

☑ Enable Keep Alive
  ☑ Try to bring up all possible Tunnels
☐ Require authentication of local users
☐ Require authentication of remote users
  ● Remote users behind VPN gateway
  ○ Remote VPN clients with XAUTH
☑ Enable Windows Networking (NetBIOS) Broadcast
☐ Apply NAT and Firewall Rules
☑ Forward packets to remote VPNs

Default LAN Gateway: 10.10.10.254

VPN Terminated at:
● LAN ○ WLAN ○ LAN/WLAN

Wireless Bridge VPN Policy

The Wireless Bridge VPN Policy is configured as follows:

1 Click **VPN**, then **Configure**.

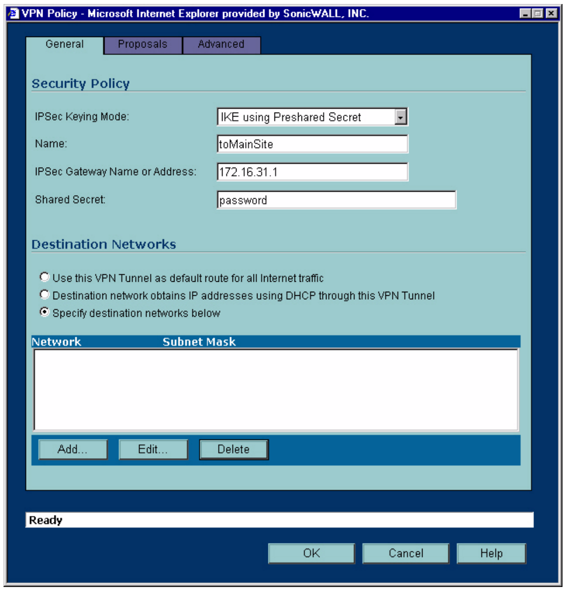
2 Select **IKE using Preshared Secret** from the **IPSec Keying Mode** menu.

3 Enter a name for the SA in the **Name** field.

4 Type the IP address of the Access Point in the **IPSec Gateway** field. In our example network, the IP address is 172.16.31.1.

5 Select **Use this VPN Tunnel as default route for all Internet traffic** from the **Destination Networks** section.

Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Network
Subnet Mask
Add...
Edit...
Delete
Ready
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret
Name: toMainSite
IPSec Gateway Name or Address: 172.16.31.1
Shared Secret: password

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel
● Specify destination networks below

CHAPTER

24

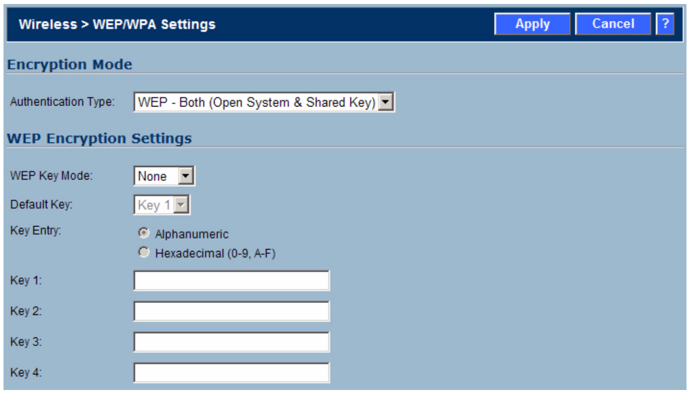
Configuring WEP and WPA Encryption

Wireless > WEP/WPA Encryption

Wired Equivalent Protocol (WEP) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWALL. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

WiFiSec should be enabled in addition to WEP for added security on the wireless network.

Wi-Fi Protected Access (WPA) provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, opposed to the static key that WEP uses.



Authentication Type: WEP - Both (Open System & Shared Key)

WEP Key Mode: None

Default Key: Key 1

Key Entry: ● Alphanumeric ○ Hexadecimal (0-9, A-F)

Key 1:

Key 2:

Key 3:

Key 4:

WEP Encryption Settings

Open-system authentication is the only method required by 802.11b. In open-system authentication, the SonicWALL allows the wireless client access without verifying its identity.

Shared-key authentication uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.

The TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless provides the option of using **Open System**, **Shared Key**, or both when WEP is used to encrypt data.

If **Both Open System & Shared Key** is selected, the **Default Key** assignments are not important as long as the identical keys are used each field. If **Shared Key** is selected, then the key assignment is important.

To configure WEP on the SonicWALL, log into the SonicWALL and click **Wireless**, then **WEP Encryption**.

1. Select the authentication type from the **Authentication Type** list. **Both (Open System & Shared Key)** is selected by default.
2. Select 64-bit or 128-bit from the **WEP Key Mode**. 128-bit is considered more secure than 64-bit. This value is applied to all keys.

WEP Encryption Keys

1. Select the key number, 1,2,3, or 4, from the **Default Key** menu.
2. Select the key type to be either **Alphanumeric** or **Hexadecimal**.

WEP - 64-bit	**WEP - 128-bit**
Alphanumeric - 5 characters (0-9, A-Z)	Alphanumeric - 13 characters (0-9, A-Z)
Hexadecimal - 10 characters (0-9, A-F)	Hexadecimal - 26 characters (0-9, A-F)

3. Type your keys into each field.
4. Click **Apply**.

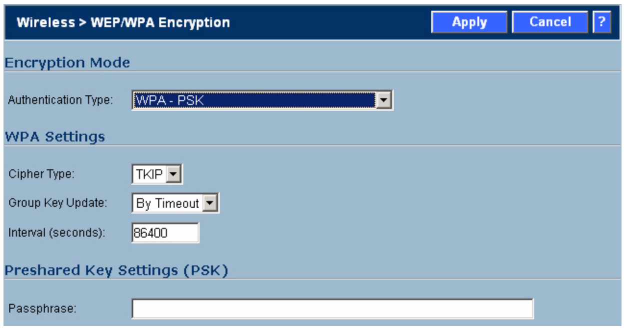
WPA Encryption Settings

WPA supports two protocols for storing and generating keys:

- *Extensible Authentication Protocol* (EAP): EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.
- *Pre-Shared Key* (PSK): PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.

Note: *WPA support is only available in Access Point Mode. WPA support is not available in Bridge Mode.*

WPA-PSK Settings


Wireless > WEP/WPA Encryption
Apply
Cancel
?
Encryption Mode
WPA Settings
Preshared Key Settings (PSK)

Authentication Type: WPA - PSK

Cipher Type: TKIP

Group Key Update: By Timeout

Interval (seconds): 86400

Passphrase:

Encryption Mode: In the **Authentication Type** field, select **WPA-PSK**.

WPA Settings:

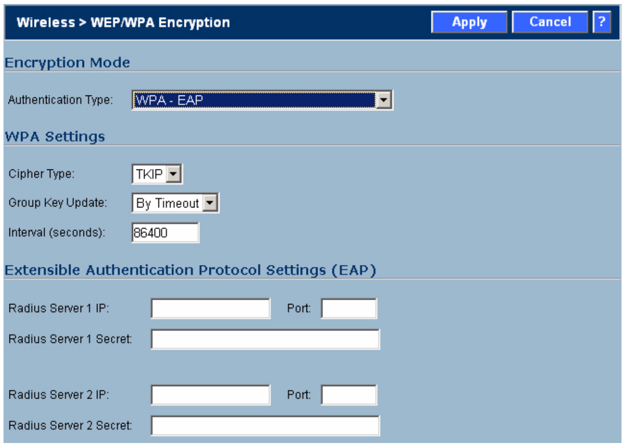
- **Cypher Type**: select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update**: Select the how to determine when to update the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval**: If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.
- **Packet Threshold**: If you selected By Packet, select the number (x 1000) of packets to pass before generating a new group key.

Preshared Key Settings (PSK)

- **Passphrase**: Enter the passphrase from which the key is generated.

Click **Apply** in the top right corner to apply your WPA settings.

WPA-EAP Settings


Wireless > WEP/WPA Encryption
Apply
Cancel
?
Encryption Mode
WPA Settings
Extensible Authentication Protocol Settings (EAP)

Authentication Type: WPA - EAP

Cipher Type: TKIP

Group Key Update: By Timeout

Interval (seconds): 86400

Radius Server 1 IP: Port:

Radius Server 1 Secret:

Radius Server 2 IP: Port:

Radius Server 2 Secret:

Encryption Mode: In the **Authentication Type** field, select **WPA-EAP**.

WPA Settings:

- **Cypher Type**: select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update**: Select the how to determine when to update the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval**: If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.
- **Packet Threshold**: If you selected By Packet, select the number (x 1000) of packets to pass before generating a new group key.

Extensible Authentication Protocol Settings (PSK)

- **Radius Server 1 IP** and **Port**: Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret**: Enter the password for access to Radius Server
- **Radius Server 2 IP** and **Port**: Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret**: Enter the password for access to Radius Server

Click **Apply** in the top right corner to apply your WPA settings.

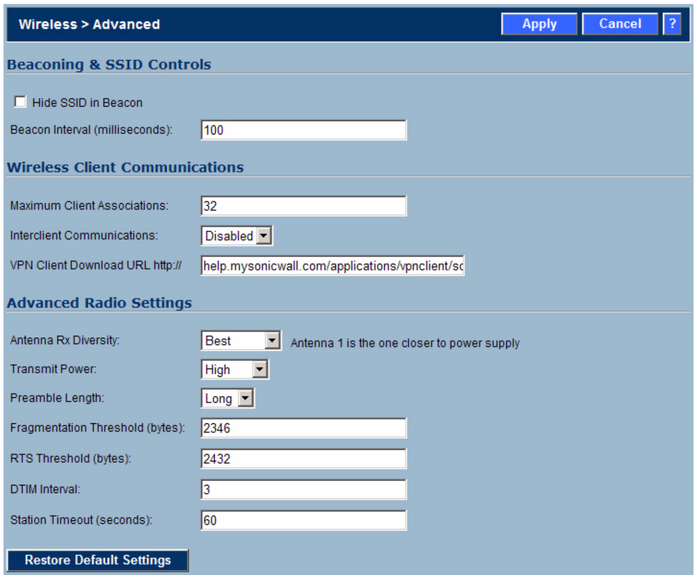
CHAPTER

25

Configuring Advanced Wireless Settings

Wireless > Advanced

To access Advanced configuration settings for the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, log into the SonicWALL, click **Wireless**, and then **Advanced**.


Wireless > Advanced
Apply
Cancel
?
Beaconing & SSID Controls
Wireless Client Communications
Advanced Radio Settings
Restore Default Settings

☐ Hide SSID in Beacon
Beacon Interval (milliseconds): 100
Maximum Client Associations: 32
Interclient Communications: Disabled
VPN Client Download URL http:// help.mysonicwall.com/applications/vpnclient/sc
Antenna Rx Diversity: Best Antenna 1 is the one closer to power supply
Transmit Power: High
Preamble Length: Long
Fragmentation Threshold (bytes): 2346
RTS Threshold (bytes): 2432
DTIM Interval: 3
Station Timeout (seconds): 60

Beaconing & SSID Controls

1. Select **Hide SSID in Beacon**. If you select **Hide SSID in Beacon**, your wireless network is invisible to anyone who does not know your SSID. This is a good way to prevent “drive by hackers” from seeing your wireless connection.
2. Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

Wireless Client Communications

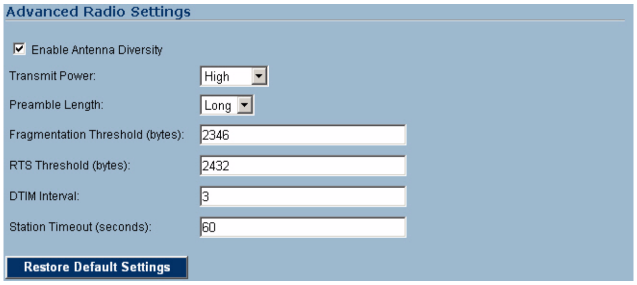
1. Enter the number of clients to associate with the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless in the **Maximum Client Associations** field. The default value is **32** which means 32 users can access the WLAN at the same time. However, an unlimited number of wireless clients can access the WLAN because node licensing does not apply to the WLAN.
2. If you do not want wireless clients communicating to each other, select **Disabled** from the **Interclient Communications** menu. If you want wireless clients communicating with each other, select **Enabled**. Enabling and disabling Interclient communications changes the associated network access rule on the **Firewall > Access Rules** page.
3. Guests on the wireless network can download the SonicWALL Global VPN Client to install on their computer or laptop. Type the URL location for the software in the **VPN Client Download URL http** field. This field can contain up to 128 characters.

Advanced Radio Settings

Configurable Antenna Diversity (TZ 170 Wireless)

The TZ 170 Wireless employs dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the TZ 170 Wireless, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal.

To allow for external (e.g. higher gain uni-directional) antennas to be used, antenna diversity can now be disabled from the **Wireless > Advanced > Advanced Radio Settings** section.



Advanced Radio Settings

☑ Enable Antenna Diversity

Transmit Power: High

Preamble Length: Long

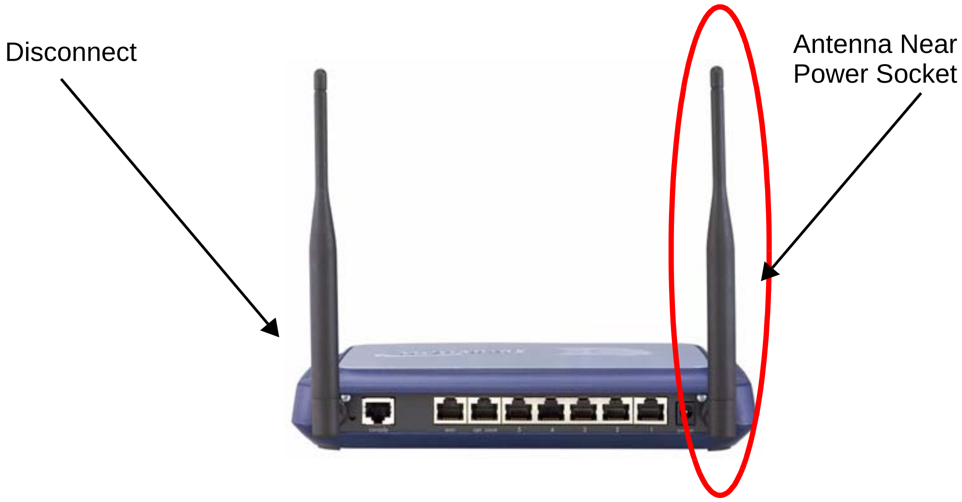
Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2432

DTIM Interval: 3

Station Timeout (seconds): 60

Clearing the **Enable Antenna Diversity** checkbox presents a pop-up message indicating that only the antenna nearest the power-socket is active when antenna diversity is disabled. The antenna nearest the serial connector **must be disconnected** when antenna diversity is disabled. The optional antenna should then be connected to the RP-TNC type connector near the power-socket. This antenna is not used exclusively for transmitting and receiving.



Select **High** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **High** if the signal is going from building to building. **Medium** is recommended for office to office within a building, and **Low** or **Lowest** is recommended for shorter distance communications.

1. Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
2. The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
3. The **RTS Threshold (bytes)** is 2432 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
4. The default value for the **DTIM Interval** is 3. Increasing the DTIM Interval value allows you to conserve power more effectively.
5. The **Station Timeout (seconds)** is 300 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Station Timeout (seconds)** field.

Click **Restore Default Settings** to return the radio settings to the default settings.

Click **Apply** in the top right corner of the page to apply your changes to the security appliance.

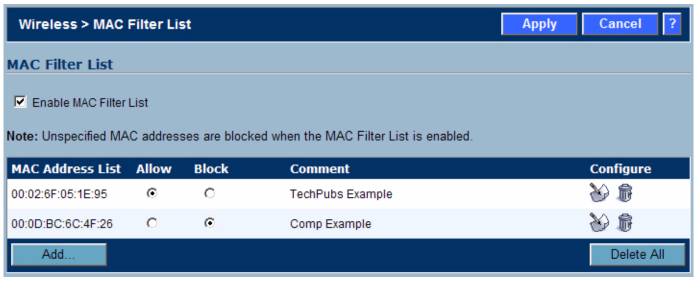
CHAPTER 26

Configuring the MAC Filter List

Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. Unless you enable **Easy WGS MAC Filtering** as a privilege when you configure a User account in **Users > Settings**.

To set up your MAC Filter List, log into the SonicWALL, and click **Wireless**, then **MAC Filter List**.



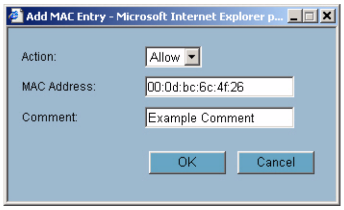
MAC Filter List

☑ Enable MAC Filter List

Note: Unspecified MAC addresses are blocked when the MAC Filter List is enabled.

MAC Address List	Allow	Block	Comment	Configure
00:02:6F:05:1E:95	●	○	TechPubs Example	
00:0D:BC:6C:4F:26	○	●	Comp Example	

1 Click **Add** to add a MAC address to the **MAC Filter List**.



Action: Allow

MAC Address: 00:0d:bc:6c:4f:26

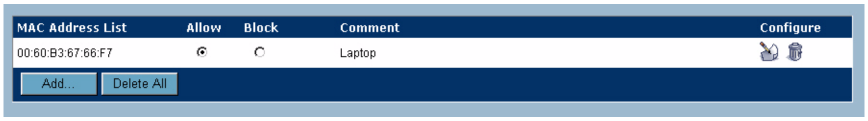
Comment: Example Comment

2 Select **Allow** from the **Action** menu to allow access to the WLAN. To deny access, select **Block**.

3 Type the MAC address in the **MAC Address** field. The two character groups should be separated by a hyphen.

4 Type a name or comment in the **Comment** field. The **Comment** field can be used to identify the source of the MAC address.

5 Click **OK** to add the MAC address.



MAC Address List	Allow	Block	Comment	Configure
00:60:B3:67:66:F7	●	○	Laptop	

Once the MAC address is added to the **MAC Address List**, you can select **Allow** or **Block** next to the entry. For example, if the user with the wireless card is not always in the office, you can select **Block** to deny access during the times the user is offsite.

Click on the Edit icon under **Configure** to edit the entry. Click on the Trashcan icon to delete the entry. To delete all entries, click **Delete All**.

CHAPTER

27

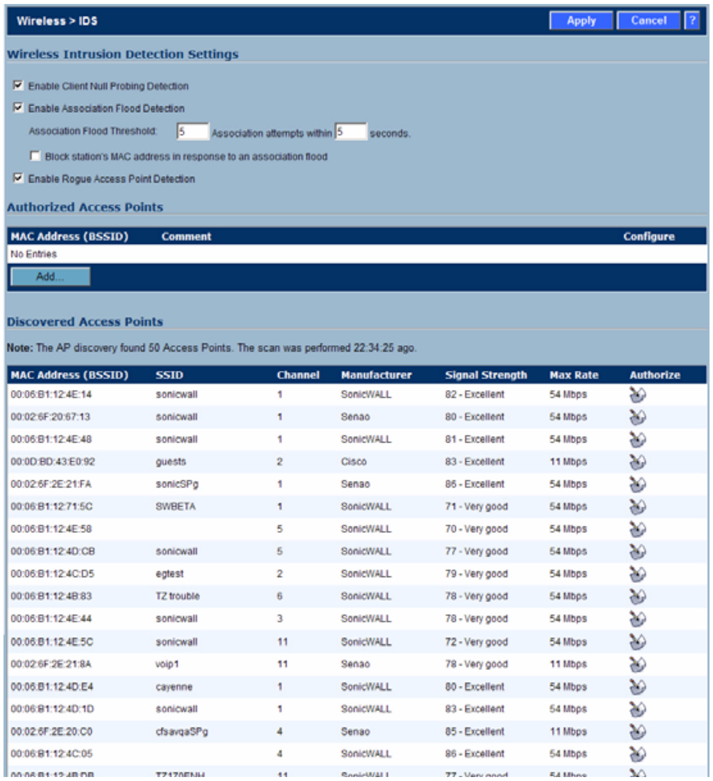
Configuring Wireless IDS

Wireless > IDS

Wireless Intrusion Detection Services (WIDS) greatly increase the security capabilities of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless by enabling it to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. WIDS logging and notification can be enabled under **Log > Categories** by selecting the **WIDS** checkbox under **Log Categories** and **Alerts**.

Wireless Bridge IDS

When the **Radio Role** of the TZ 170 Wireless is set to a Wireless Bridge mode, Rogue Access Point Detection defaults to active mode (actively scanning for other Access Points using probes on all channels).



☑ Enable Client Null Probing Detection

☑ Enable Association Flood Detection

Association Flood Threshold: 5 Association attempts within 5 seconds.

☐ Block station's MAC address in response to an association flood

☑ Enable Rogue Access Point Detection

MAC Address (BSSID)	Comment	Configure
No Entries		

Note: The AP discovery found 50 Access Points. The scan was performed 22:34:25 ago.

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:06:B1:12:4E:14	sonicwall	1	SonicWALL	82 - Excellent	54 Mbps	
00:02:6F:20:67:13	sonicwall	1	Senao	80 - Excellent	54 Mbps	
00:06:B1:12:4E:48	sonicwall	1	SonicWALL	81 - Excellent	54 Mbps	
00:0D:BD:43:E0:92	guests	2	Cisco	83 - Excellent	11 Mbps	
00:02:6F:2E:21:FA	sonicSPg	1	Senao	86 - Excellent	54 Mbps	
00:06:B1:12:71:5C	SWBETA	1	SonicWALL	71 - Very good	54 Mbps	
00:06:B1:12:4E:58		5	SonicWALL	70 - Very good	54 Mbps	
00:06:B1:12:4D:CB	sonicwall	5	SonicWALL	77 - Very good	54 Mbps	
00:06:B1:12:4C:D5	egtest	2	SonicWALL	79 - Very good	54 Mbps	
00:06:B1:12:4B:83	TZ trouble	6	SonicWALL	78 - Very good	54 Mbps	
00:06:B1:12:4E:44	sonicwall	3	SonicWALL	78 - Very good	54 Mbps	
00:06:B1:12:4E:5C	sonicwall	11	SonicWALL	72 - Very good	54 Mbps	
00:02:6F:2E:21:8A	voip1	11	Senao	78 - Very good	11 Mbps	
00:06:B1:12:4D:E4	cayenne	1	SonicWALL	80 - Excellent	54 Mbps	
00:06:B1:12:4D:1D	sonicwall	1	SonicWALL	83 - Excellent	54 Mbps	
00:02:6F:2E:20:C0	cfsavqaSPg	4	Senao	85 - Excellent	11 Mbps	
00:06:B1:12:4C:05		4	SonicWALL	86 - Excellent	54 Mbps	

Access Point IDS

When the **Radio Role** of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to perform an active scan, and may cause a brief loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Enable Client Null Probing

The control to block Null probes is not available on the 802.11g card built into the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. Instead, enabling this setting allows the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to detect and log Null Probes, such as those used by Netstumbler and other similar tools.

Association Flood Detection

Association Flood is a type of Wireless Denial of Service attack intended to interrupt wireless services by depleting the resources of a wireless Access Point. An attacker can employ a variety of tools to establish associations, and consequently association IDs, with an access point until it reaches its association limit (generally set to 255). Once association saturation occurs, the access point discards further association attempts until existing associations are terminated.

Association Flood Detection allows thresholds to be set limiting the number of association attempts a client makes in a given span of time before its activities are considered hostile. Association attempts default to a value of 5 (minimum value is 1, maximum value is 100) within and the time period defaults to a value of 5 seconds (minimum value is 1 second, maximum value is 999 seconds). If association attempts exceed the set thresholds, an event is logged according to log settings.

If the **Block station's MAC address in response to an association flood** option is selected and MAC Filtering is enabled, then in addition to logging actions, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless takes the countermeasure of dynamically adding the MAC address to the MAC filter list. Any future Denial of Service attempts by the attacker are then blocked.

Enable Association Flood Detection is selected by default. The **Association Flood Threshold** is set to **5 Association attempts within 5 seconds** by default.

Rogue Access Point Detection

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11b channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

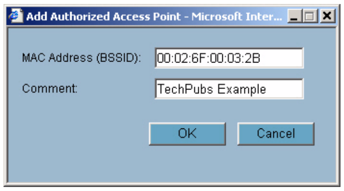
Active scanning occurs when the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless starts up, and at any time **Scan Now** is clicked on the **Wireless > IDS** page. When the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

Alert: *The **Scan Now** feature causes a brief disruption in service. If this is a concern, wait and use the **Scan Now** feature at a time when no clients are active, or the potential for disruption becomes acceptable.*

Authorizing Access Points on Your Network

Access Points detected by the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless are regarded as rogues until they are identified to the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless as authorized for operation. To authorize an access point, it can be manually added to the **Authorized Access Points** list by clicking **Add** and specifying its MAC address (BSSID) along with an optional comment.



MAC Address (BSSID): 00:02:6F:00:03:2B

Comment: TechPubs Example

Alternatively, if an access point is discovered by the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless scanning feature, it can be added to the list by clicking the **Authorize** icon.

PART

6

Wireless Guest Services

CHAPTER

28

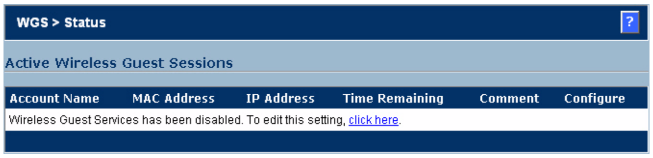
Viewing Wireless Guest Services Status

Wireless Guest Services (WGS) allow you to create access accounts for temporary use that allow wireless clients to connect from the WLAN to the WAN.

WGS > Status

The **WGS > Status** page displays the **Active Wireless Guest Sessions**. The table lists the **Account Name**, **MAC Address**, **IP Address**, **Time Remaining**, and **Comment**. The last column, **Configure**, allows you to make changes to the guest account when you click the **Configure** icon next to the account.

If Wireless Guest Services are not enabled, Click the link in the **Status** page to enable the services.



Account Name	MAC Address	IP Address	Time Remaining	Comment	Configure
Wireless Guest Services has been disabled. To edit this setting, click here.					

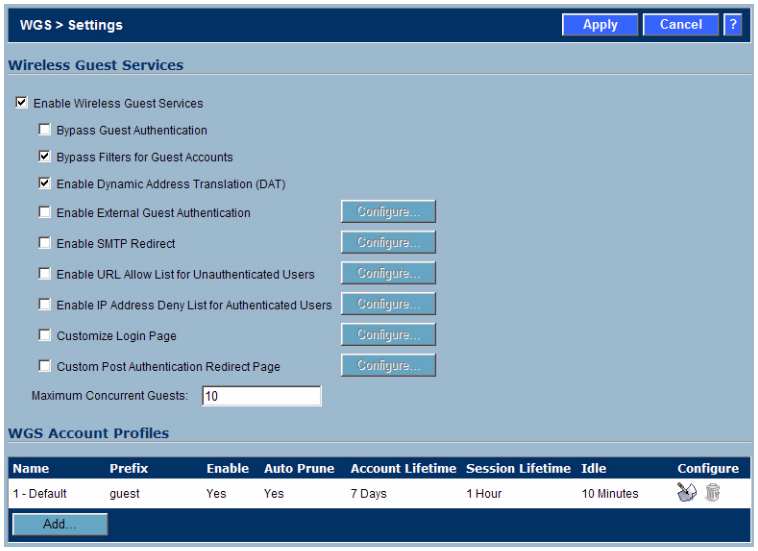
CHAPTER 29

Configuring Wireless Guest Services

Wireless Guest Services (WGS) allow you to create access accounts for temporary use that allow wireless clients to connect from the WLAN to the WAN.

WGS > Settings

The **WGS > Settings** page allows you to configure wireless guest services on your TZ 50 Wireless/ TZ 150 Wireless/TZ 170 Wireless.



Wireless Guest Services

☑ Enable Wireless Guest Services
  ☐ Bypass Guest Authentication
  ☑ Bypass Filters for Guest Accounts
  ☑ Enable Dynamic Address Translation (DAT)
  ☐ Enable External Guest Authentication
  ☐ Enable SMTP Redirect
  ☐ Enable URL Allow List for Unauthenticated Users
  ☐ Enable IP Address Deny List for Authenticated Users
  ☐ Customize Login Page
  ☐ Custom Post Authentication Redirect Page

Maximum Concurrent Guests: 10

WGS Account Profiles

Name	Prefix	Enable	Auto Prune	Account Lifetime	Session Lifetime	Idle	Configure
1 - Default	guest	Yes	Yes	7 Days	1 Hour	10 Minutes	

Check **Enable Wireless Guest Services** to enable wireless guest service access to the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wirelessnetwork.

Bypass Guest Authentication

Bypass Guest Authentication allows a TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is enforcing authentication.

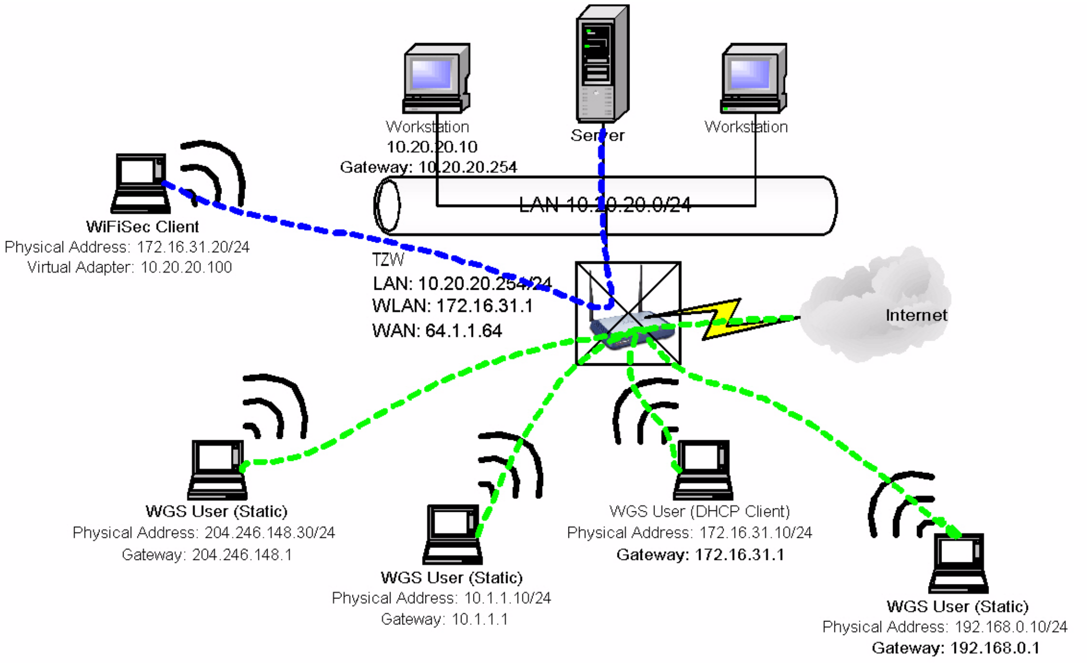
Bypass Filters for Guest Accounts

Bypass Filters for Guest Accounts disables the SonicWALL Content Filtering Service for guests. Use this if your network is protected by content filtering somewhere between the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless and the Internet, or if you want to provide unrestricted internet access to your guests. See **Chapter 43, Managing SonicWALL Security Services** for more information about content filtering.

Enable Dynamic Address Translation (DAT)

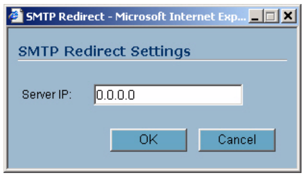
One of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless key features is Wireless Guest Services (WGS), which provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, WGS allows wireless users to authenticate and associate, obtain IP settings from the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless DHCP services, and authenticate using any web-browser. Without DAT, if a WGS user is not a DHCP client, but instead has static IP settings incompatible with the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values.

Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support any IP addressing scheme for WGS users. For example, the TZ 150 Wireless/TZ 170 Wireless WLAN interface is configured with its default address of 172.16.31.1, and one WGS client has a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.


Workstation
10.20.20.10
Gateway: 10.20.20.254
Server
Workstation
LAN 10.20.20.0/24
WiFiSec Client
Physical Address: 172.16.31.20/24
Virtual Adapter: 10.20.20.100
TZW
LAN: 10.20.20.254/24
WLAN: 172.16.31.1
WAN: 64.1.1.64
Internet
WGS User (Static)
Physical Address: 204.246.148.30/24
Gateway: 204.246.148.1
WGS User (Static)
Physical Address: 10.1.1.10/24
Gateway: 10.1.1.1
WGS User (DHCP Client)
Physical Address: 172.16.31.10/24
Gateway: 172.16.31.1
WGS User (Static)
Physical Address: 192.168.0.10/24
Gateway: 192.168.0.1

Enable SMTP Redirect

Enable SMTP Redirect causes SMTP traffic coming in from a guest account to be redirected to the SMTP server you specify. Check **Enable SMTP Redirect** and click the **Configure** button in the same line. In the SMTP Redirect Settings window, enter the IP address of the SMTP server.


SMTP Redirect - Microsoft Internet Exp...
SMTP Redirect Settings
OK
Cancel

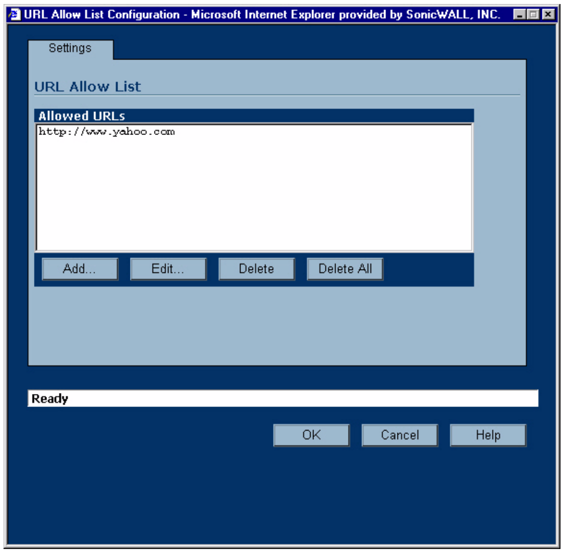
Server IP: 0.0.0.0

Enable URL Allow List for Authenticated Users

Enable URL Allow List for Unauthenticated Users, when selected, allows for the creation of a list of URLs (HTTP and HTTPS only) that WGS users can visit even before they authenticate. This feature could be used, for example, to allow users to reach advertising pages, disclaimer pages, search engines, etc. Entries should be made in URL format, and can be in either Fully Qualified Domain Name (FQDN) or IP address syntax.

1 Select **Enable URL Allow List for Unauthenticated Users**.

2 Click **Configure** to display the **URL Allow List Configuration** window.


URL Allow List Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
URL Allow List
Allowed URLs
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

http://www.yahoo.com

Ready

3 Click **Add** to display the **Add URL** dialogue box.

4 Enter the URL in http or https format or domain name. For instance, http://www.yahoo.com or yahoo.com. Click **OK**, then **OK** again.

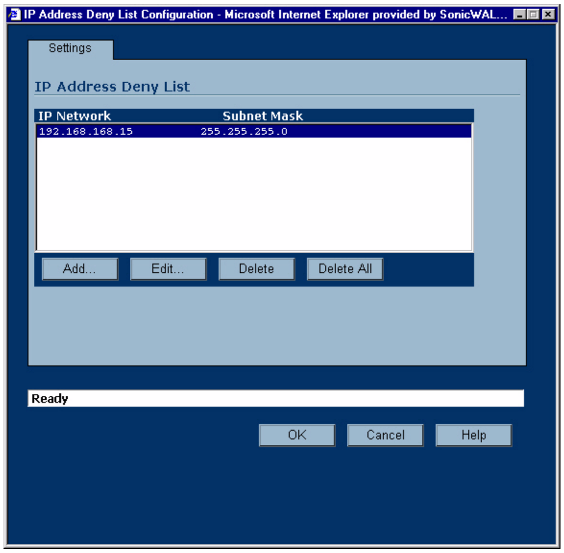
✓ **Tip:** *Up to 32 entries consisting of 128 characters each can be added to the* TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless*.*

Enable IP Address Deny List for Authenticated Users

When **Enable IP Address Deny List for Authenticated Users** is selected, allows for the specification of IP addresses/subnet masks to which WGS users are explicitly denied access. Individual hosts can be entered by using a 32 bit subnet mask (255.255.255.255), networks can be entered with appropriate subnet mask, or network ranges can be aggregated using CIDR notation or supernetting (e.g. entering 192.168.0.0/255.255.240.0 to cover individual class C networks 192.168.0.0/24 through 192.168.15.0/24).

1 Select **Enable IP Address Deny List for Authenticated Users**.

2 Click **Configure**.


IP Address Deny List Configuration - Microsoft Internet Explorer provided by SonicWAL...
Settings
IP Address Deny List
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

IP Network	Subnet Mask
192.168.168.15	255.255.255.0

Ready

3 Click **Add** to display the **Add IP Address Deny List Entry** window.

4 Type the IP Address in the **IP Network** field. Type the subnet mask in the **Subnet Mask** field.

5 Click **OK**. Then click **OK** again.

The IP address or network range is added to the list.

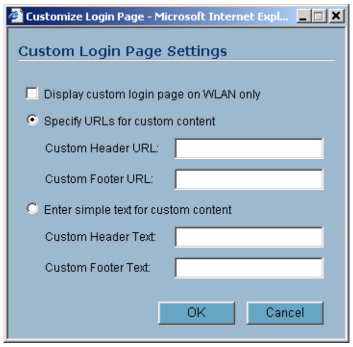
✓ **Tip:** *Up to 32 entries consisting of 128 characters each can be added to the TZ 150 Wireless/TZ 170 Wireless.*

Customize Login Page

Customize Login Page allows you to display a custom login page to guest users when they first log into the TZ 170. The custom login page is constructed from a header and footer you specify and entry fields for guest user name and password between the header and footer. To configure a custom login page:

1 Check the **Customize Login Page** box.

2 Click **Configure** to open the Custom Login Page Settings window


Customize Login Page - Microsoft Internet Expl...
Custom Login Page Settings
OK
Cancel

☐ Display custom login page on WLAN only

● Specify URLs for custom content

Custom Header URL:

Custom Footer URL:

○ Enter simple text for custom content

Custom Header Text:

Custom Footer Text:

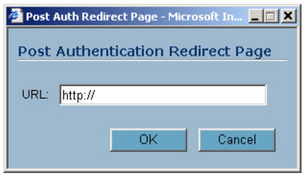
3 Check **Display custom login page on WLAN only** to restrict only wireless guests to this page. Leave it unchecked to display it to all guest users.

4. Select **Specify URLs for custom content** if you have graphics or text available on a web server to use at the header and footer of the login page. Enter the URLs for the content in the **Custom Header URL** and **Custom Footer URL** fields.
5. Select **Enter simple text for custom content** to enter the header and footer text for the login page directly. Enter the text in the **Custom Header Text** and **Custom Footer Text** fields.
6. Click OK to save these entries.

Custom Post Authentication Redirect Page

Custom **Post Authentication Redirect Page** redirects the users to a web page you specify upon successful log in and authentication.

1. Check **Custom Post Authentication Redirect Page**.
2. Click **Configure** to display the **Post Authentication Redirect Page** window.
3. Enter the URL of the redirect page in the **URL** field and click OK.


Post Auth Redirect Page - Microsoft In...
Post Authentication Redirect Page
URL:
OK
Cancel

URL: http://

Maximum Concurrent Guests

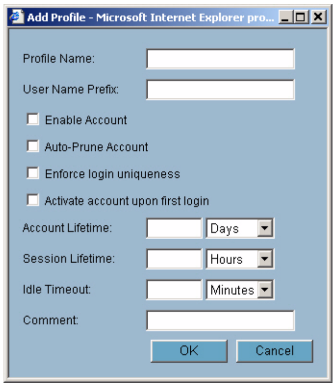
You can restrict the number of concurrent guests on your TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. Enter the maximum number of guests in the **Maximum Concurrent Guests field**. Click **Apply** at the top right corner of this page to enact this setting.

WGS Account Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles.

To add a profile:

1. Click **Add** below the Guest Profile list to display the Add Guest Profile window.


Add Profile - Microsoft Internet Explorer pro...
Profile Name:
User Name Prefix:
☐ Enable Account
☐ Auto-Prune Account
☐ Enforce login uniqueness
☐ Activate account upon first login
Account Lifetime:
Days
Session Lifetime:
Hours
Idle Timeout:
Minutes
Comment:
OK
Cancel

2. In the Add Guest Profile window, configure:
   - **Profile Name**: Enter the name of the profile.
   - **User Name Prefix**: Enter the first part of every user account name generated from this profile.

- **Enable Account**: Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account**: Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness**: Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.
- **Activate account upon first login**: Check this for the account to remain inactive until the user logs in and activates the account.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment**: Any text can be entered as a comment in the **Comment** field.

3 Click **OK** to add the profile.

CHAPTER 30

Managing Wireless Guest Accounts

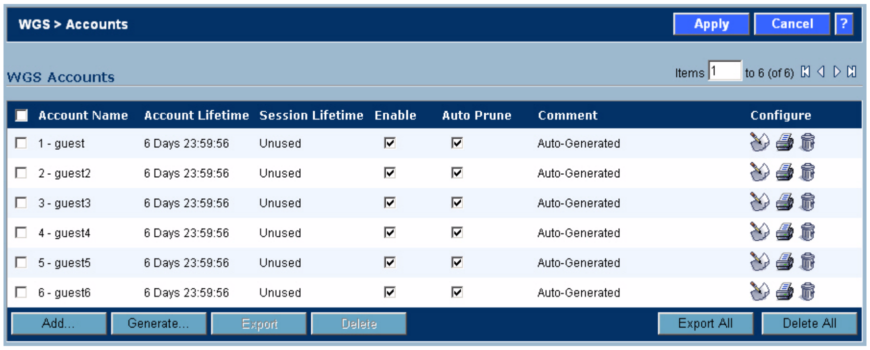
Wireless Guest Services (WGS) allow you to create access accounts for temporary use that allow wireless clients to connect from the WLAN to the WAN.

WGS > Accounts

The task of generating a new WGS account is now easier with the introduction of an automated account generation function with the ability to generate (or re-generate) account name and account password information.

Working with Guest Accounts

To disable a Guest Account, clear the **Enable** check box in the Guest Account entry line. To edit an existing Guest Account, click on the Notepad icon under **Configure.** To delete a Guest Account, click the Trashcan icon under **Configure**. To delete all Guest Accounts, click **Delete All**.

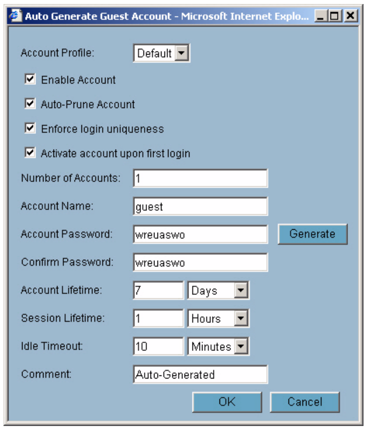


☐	Account Name	Account Lifetime	Session Lifetime	Enable	Auto Prune	Comment	Configure
☐	1 - guest	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	
☐	2 - guest2	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	
☐	3 - guest3	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	
☐	4 - guest4	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	
☐	5 - guest5	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	
☐	6 - guest6	6 Days 23:59:56	Unused	☑	☑	Auto-Generated	

Automatically Generating Guest Accounts

You can generate a specified number of guest accounts.

1. Under the list of accounts, click **Generate**.



Account Profile: Default
☑ Enable Account
☑ Auto-Prune Account
☑ Enforce login uniqueness
☑ Activate account upon first login
Number of Accounts: 1
Account Name: guest
Account Password: wreuaswo
Confirm Password: wreuaswo
Account Lifetime: 7 Days
Session Lifetime: 1 Hours
Idle Timeout: 10 Minutes
Comment: Auto-Generated

2. In the Auto Generate Guest Account window, configure the settings for all the accounts you are generating:
   - **Profile**: Select the Guest Profile to generate the accounts from.Number of Accounts:
   - **Enable Account**: Check this for the accounts to be enabled upon creation.
   - **Auto-prune Account**: Check this to have the account removed from the database after its lifetime expires.
   - **Enforce login uniqueness**: Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
   - **Activate account upon first login**: Check this option to make this account active when the user first logs in to WGS.
   - **Number of Accounts**: Enter the number of accounts to generate.
   - **Account Name**: Enter a name for the accounts. If you generate more than one account at a time, a number will be added at the end of each account name to make the name unique.
   - **Account Password**: The password is automatically generated by default. If you do not want to use the generated password, enter a new one, and confirm it in the **Confirm Password** field, or click **Generate** to generate a new password.
   - **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
   - **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
   - **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.
   - **Comment**: Enter a descriptive comment.
3. Click **OK** to generate the accounts.

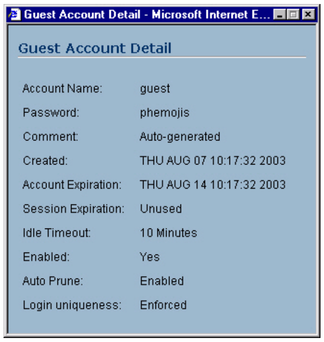
Manually Configuring Wireless Guests

To configure new wireless guest accounts, click **Add**. The **Add Guest Account** window is displayed.

- **Account Profile**:
- The following settings are enabled by default:
- **Enable Account**: When selected, the wireless guest account is automatically enabled. You can clear the checkbox to disable the account until necessary.
- **Auto-Prune Account**: By default, newly created accounts are set to **Auto-Prune**, automatically deleted when expired. If **Auto-Prune** is cleared, the account remains in the list of WGS accounts with an **Expired** status, allowing it to be easily reactivated.
- **Enforce login uniqueness**: By enforcing login uniqueness, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless allows only a single instance of a WGS account to be used at any one time. By default, this feature is enabled when creating a new WGS account. If you want to allow multiple users to login with a single account, this enforcement is disabled by clearing the **Enforce login uniqueness** checkbox.
- **Activate account upon first login**: By default, the Activate Account Upon First Login is enabled on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless. The WGS account remains inactive until the user logs in and activates the account.
- **Account Name**: Generate
- **Account Password**: Generate
- **Confirm Password**:
- **Account Lifetime**: This setting defines how long an account remains on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless before the account expires. If **Auto-Prune** is enabled, the account is deleted by the SonicWALL security appliance. If the **Auto-Prune** checkbox is cleared, the account remains in the list of WGS accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime**: Defines how long a WGS session remains active after it has been activated. By default, activation occurs the first time a WGS user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated WGS session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment**: Any text can be entered as a comment in the **Comment** field.

Account Detail Printing

Following the generation of an account, it is possible to click the **Print** icon on the **WGS > Settings** page to send the pertinent account details to the active printer on the administrative workstation for easy distribution to WGS users. Clicking the **Print** icon launches the following window, followed by the administrative workstation's system print dialog.



Guest Account Detail

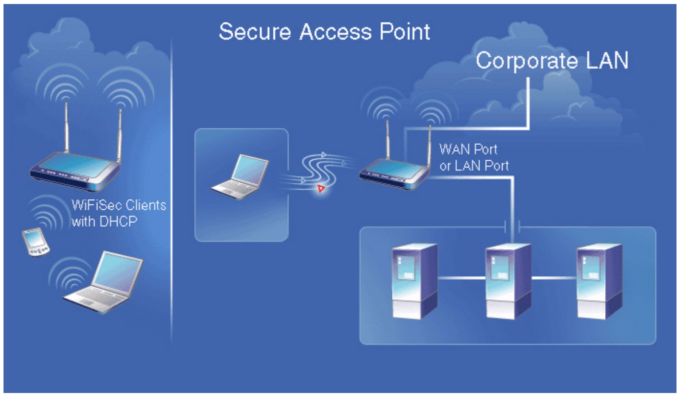
Account Name:	guest
Password:	phemojis
Comment:	Auto-generated
Created:	THU AUG 07 10:17:32 2003
Account Expiration:	THU AUG 14 10:17:32 2003
Session Expiration:	Unused
Idle Timeout:	10 Minutes
Enabled:	Yes
Auto Prune:	Enabled
Login uniqueness:	Enforced

Flexible Default Route

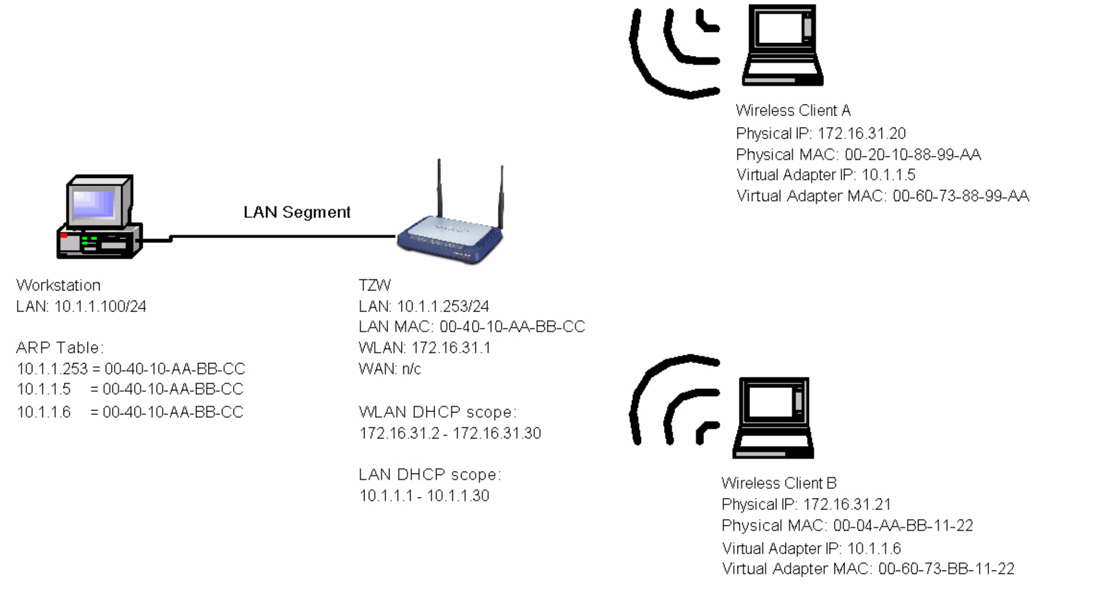
Previously, network traffic from the LAN and WLAN was directed to the WAN interface. With the release of SonicOS Standard, the Default Route can be the WAN, LAN, or WLAN allowing flexible configuration of the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless, primarily wireless bridging without WiFiSec and Secure Access Point with Virtual Adapter support.

Secure Access Point with Virtual Adapter Support

Secure Access Point deployment previously required the corporate LAN to be connected to the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless WAN port, because the default route could only be specified on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless WAN interface. However, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless could not support Wireless Guest Services and SonicWALL Global VPN Clients simultaneously preventing corporate LAN clients from communicating with WLAN clients, inhibiting crucial functions such as wireless print servers, Microsoft Outlook mail notification, or any other function requiring LAN initiated communications to WLAN clients.

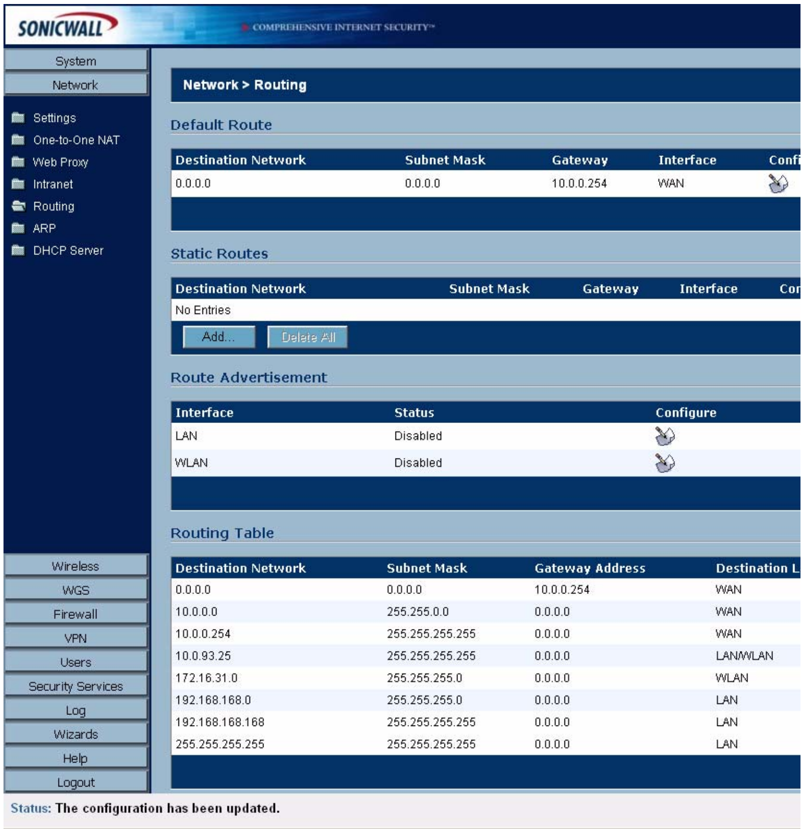

Secure Access Point
Corporate LAN
WAN Port
or LAN Port
WiFiSec Clients
with DHCP

Any LAN clients attempting to resolve an IP address of a Global VPN Virtual Adapter address receives a response from the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless LAN.


Wireless Client A
Physical IP: 172.16.31.20
Physical MAC: 00-20-10-88-99-AA
Virtual Adapter IP: 10.1.1.5
Virtual Adapter MAC: 00-60-73-88-99-AA
LAN Segment
Workstation
LAN: 10.1.1.100/24
ARP Table:
10.1.1.253 = 00-40-10-AA-BB-CC
10.1.1.5 = 00-40-10-AA-BB-CC
10.1.1.6 = 00-40-10-AA-BB-CC
TZW
LAN: 10.1.1.253/24
LAN MAC: 00-40-10-AA-BB-CC
WLAN: 172.16.31.1
WAN: n/c
WLAN DHCP scope:
172.16.31.2 - 172.16.31.30
LAN DHCP scope:
10.1.1.1 - 10.1.1.30
Wireless Client B
Physical IP: 172.16.31.21
Physical MAC: 00-04-AA-BB-11-22
Virtual Adapter IP: 10.1.1.6
Virtual Adapter MAC: 00-60-73-BB-11-22

This allows any client on the LAN to communicate directly with WLAN client via the secure WiFiSec link, enabling configurations like the one below.

To configure routing on the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless to support the above example, click **Network** and then **Routing**.



SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Wireless
WGS
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout

Network > Routing

Default Route

Destination Network	Subnet Mask	Gateway	Interface	Confi
0.0.0.0	0.0.0.0	10.0.0.254	WAN	

Static Routes

Destination Network	Subnet Mask	Gateway	Interface	Cor
No Entries				

Add...
Delete All

Route Advertisement

Interface	Status	Configure
LAN	Disabled	
WLAN	Disabled	

Routing Table

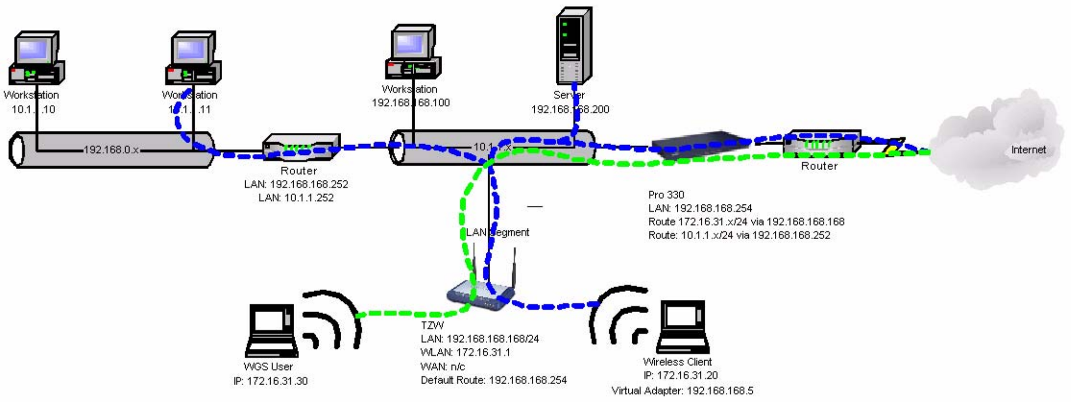
Destination Network	Subnet Mask	Gateway Address	Destination L
0.0.0.0	0.0.0.0	10.0.0.254	WAN
10.0.0.0	255.255.0.0	0.0.0.0	WAN
10.0.0.254	255.255.255.255	0.0.0.0	WAN
10.0.93.25	255.255.255.255	0.0.0.0	LAN/WLAN
172.16.31.0	255.255.255.0	0.0.0.0	WLAN
192.168.168.0	255.255.255.0	0.0.0.0	LAN
192.168.168.168	255.255.255.255	0.0.0.0	LAN
255.255.255.255	255.255.255.255	0.0.0.0	LAN

Status: The configuration has been updated.

1. Under **Default Route**, click **Configure**. The **Edit Default Route** window is displayed.
2. Enter the IP address in the **Default Gateway** field, and then select **LAN**, **WAN**, or **WLAN** from the **Interface** menu.
3. Click **OK**. The default gateway is now configured.

Secure Access Point with Wireless Guest Services

If simultaneous Wireless Guest Services support is a requirement, then access to the 172.16.31.x network is necessary. The following diagram portrays such a configuration, and also allows for an introduction to one of the WGS enhancements of SonicOS 2.0, explicit WGS allow and deny lists.



Workstation
10.1. .10
Workstation
1 .1. .11
Workstation
192.168. 68.100
Server
192.168. 68.200
192.168.0.x
Router
LAN: 192.168.168.252
LAN: 10.1.1.252
10.1. .x
Router
Internet
Pro 330
LAN: 192.168.168.254
Route 172.16.31.x/24 via 192.168.168.168
Route: 10.1.1.x/24 via 192.168.168.252
LAN Segment
TZW
LAN: 192.168.168.168/24
WLAN: 172.16.31.1
WAN: n/c
Default Route: 192.168.168.254
WGS User
IP: 172.16.31.30
Wireless Client
IP: 172.16.31.20
Virtual Adapter: 192.168.168.5

The example above describes a moderately complex network configuration where the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless offers both WiFiSec and WGS access via a default route on LAN. As the blue (WiFiSec) and green (WGS) traffic lines indicate, the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless allows WGS access only to the Internet, while allowing WiFiSec access to the Internet, the LAN, and to a remote network connected via a LAN router. The SonicWALL PRO 2040 in above example requires static routes to the 10.1.1.x (adjacent) network via 192.168.168.252, and to the 172.16.31.x (for WGS) network via 192.168.168.168.

Prior to SonicOS 1.5.0.0, Wireless Guest Services were only available in default route on WAN configurations. This scheme provided an automatic differentiation of destinations for WGS traffic. In other words, WGS traffic bound for the WAN was permitted, but WGS traffic attempting to reach the LAN (local traffic), to cross the LAN (to reach an adjacent network connected via a router) or to cross a VPN tunnel was dropped.

When the TZ 50 Wireless/TZ 150 Wireless/TZ 170 Wireless is configured to provide both Secure Access Point and WGS services via a default route on LAN, all traffic exits the LAN interface, eliminating any means of automatically classifying “WGS permissible” traffic. To address this ambiguity, any traffic sourced from a WGS client attempting to reach the default gateway (in our above example, 192.168.168.254) is allowed, but any traffic attempting to traverse a VPN, or reach a LAN resource (for example, 192.168.168.100) is dropped. Finally, to safeguard adjacent networks attached via a router, a WGS **IP Address Deny List** has been added to the **WGS > Settings** page.

PART 7

Firewall

CHAPTER 31

Configuring Network Access Rules

Network Access Rules Overview

Network Access Rules are management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL.

By default, the SonicWALL's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet rule enabled in the SonicWALL:

- Allow all sessions originating from the LAN, OPT, DMZ, or WLAN to the WAN
- Deny all sessions originating from the WAN to the LAN, OPT, DMZ, or WLAN

Additional Network Access Rules can be defined to extend or override the default rules. For example, rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

The custom rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to rules created on the SonicWALL. Network Access Rules take precedence, and can override the SonicWALL stateful packet inspection. For example, a rule that blocks IRC traffic takes precedence over the SonicWALL default setting allowing this type of traffic.

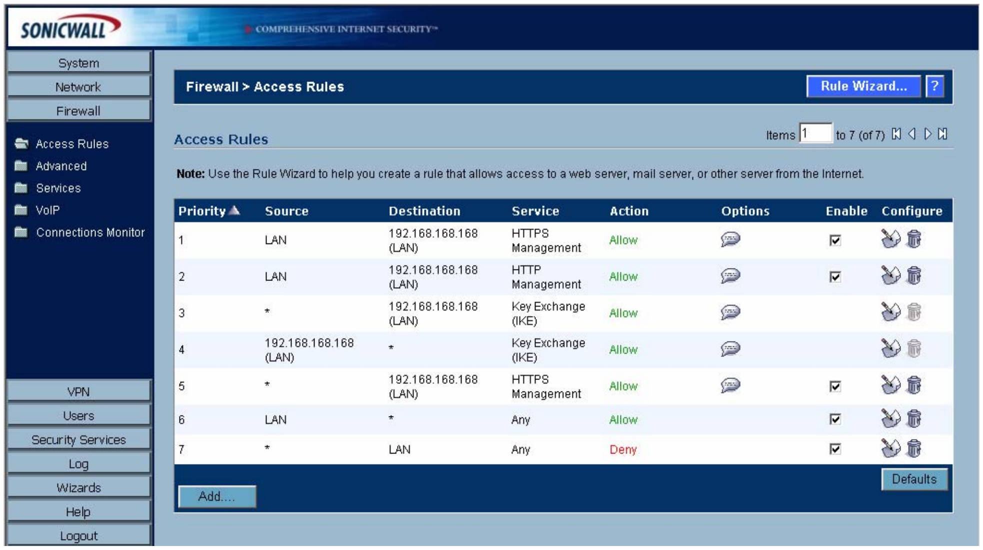
▲ **Alert:** *The ability to define Network Access Rules is a very powerful tool. Using custom rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting Network Access Rules.*

Using Bandwidth Management with Access Rules

Bandwidth management allows you to assign guaranteed and maximum bandwidth to services and also set priorities for outbound traffic. Bandwidth management only applies to **outbound** traffic from the SonicWALL to the WAN or any other destination. The minimum guaranteed bandwidth in Kbps is 20 and the maximum is 100,000 kbps. Any rule using bandwidth management has a higher priority than rules not using bandwidth management. Rules using bandwidth management based the assigned priority and rules without bandwidth management are given lowest priority. For instance, if you create a rule for outbound mail traffic (SMTP) and enable Bandwidth Management with a guaranteed bandwidth of 20 Kbps and a maximum bandwidth of 40 Kbps, priority of 0, outbound SMTP traffic always has 20 Kbps available to it and can get as much as 40 Kbps. If this is the only rule using Bandwidth Management, it has priority over all other rules on the SonicWALL. Other rules use the leftover bandwidth minus 20 Kbps (guaranteed) or minus 40 Kbps (maximum).

Alert: *You must select Bandwidth Management on the **WAN > Ethernet** tab. Click **Network**, then **Configure** in the **WAN** line of the **Interfaces** table, and enter your available bandwidth in the **Available WAN Bandwidth (Kbps**) field.*

Firewall > Access Rules



Note: Use the Rule Wizard to help you create a rule that allows access to a web server, mail server, or other server from the Internet.

Priority	Source	Destination	Service	Action	Options	Enable	Configure
1	LAN	192.168.168.168 (LAN)	HTTPS Management	Allow		☑	
2	LAN	192.168.168.168 (LAN)	HTTP Management	Allow		☑	
3	*	192.168.168.168 (LAN)	Key Exchange (IKE)	Allow			
4	192.168.168.168 (LAN)	*	Key Exchange (IKE)	Allow			
5	*	192.168.168.168 (LAN)	HTTPS Management	Allow		☑	
6	LAN	*	Any	Allow		☑	
7	*	LAN	Any	Deny		☑	

The **Access Rules** page displays a table of defined Network Access Rules. Rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Default** rule. The Default rule is all IP services except those listed in the **Access Rules** page. Rules can be created to override the behavior of the **Default** rule; for example, the **Default** rule allows users on the LAN to access all Internet services, including NNTP News.

You can enable or disable Network Access Rules by selecting or clearing the check box in the **Enable** column. Clicking the edit icon allows you to edit an existing rule, or clicking the delete icon deletes an existing rule. If the two icons are unavailable, the rule cannot be changed or removed from the list. Rules with a funnel icon are using bandwidth management.

Tip: *You can easily create Network Access Rules using the **Network Access Rule Wizard**.*

Navigating and Sorting the Access Rules Table Entries

The **Access Rules** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Access Rules** table by using the navigation control bar located at the top right of the **Access Rules** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Restoring Default Network Access Rules

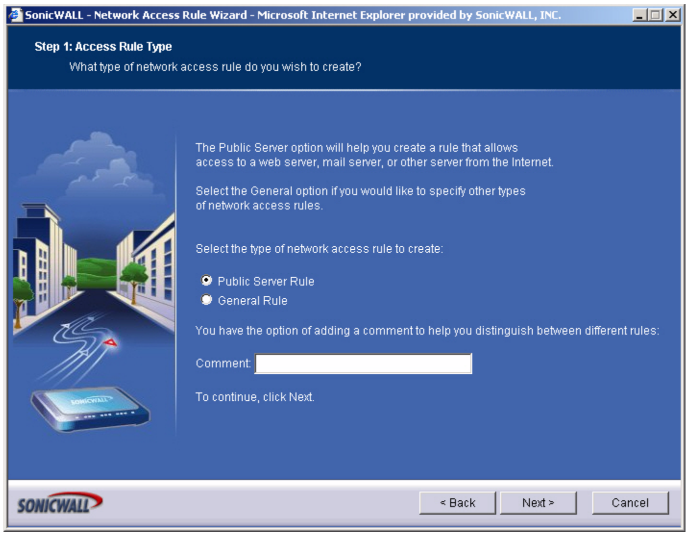
The SonicWALL includes a set of default Network Access Rules, which are listed in the **Access Rules** table. You can reset the SonicWALL at any time to restore the Network Access Rules to just the default rules by clicking on the **Defaults** button.

Adding Rules using the Network Access Rule Wizard

The **Network Access Rule Wizard** takes you step by step through the process of creating network access rules and public server rule on the SonicWALL.

Configuring a Public Server Rule

1 Click the **Rule Wizard** button at the top right of the **Firewall > Access Rules** page. Click **Next**.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 1: Access Rule Type

What type of network access rule do you wish to create?

The Public Server option will help you create a rule that allows access to a web server, mail server, or other server from the Internet.

Select the General option if you would like to specify other types of network access rules.

Select the type of network access rule to create:

● Public Server Rule
○ General Rule

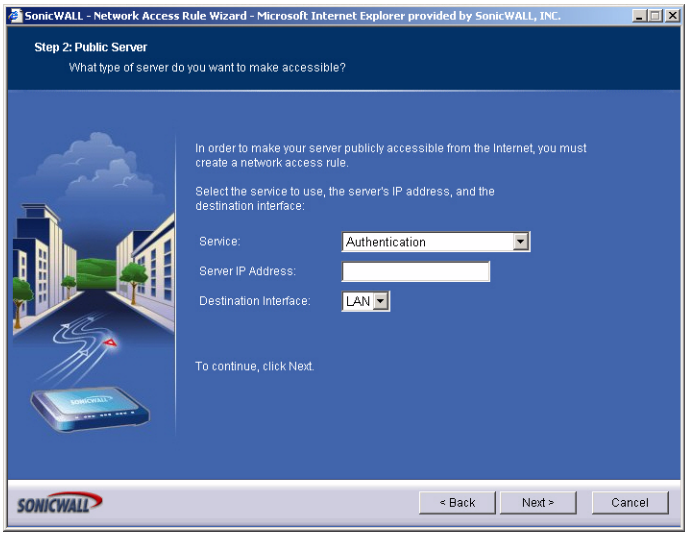
You have the option of adding a comment to help you distinguish between different rules:

Comment:

To continue, click Next.

2 Select **Public Server Rule**. Click **Next**.

3 You can add an optional text in the **Comment** field. This information is displayed in the **Options** column of the **Access Rules** table. Click **Next**.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 2: Public Server

What type of server do you want to make accessible?

In order to make your server publicly accessible from the Internet, you must create a network access rule.

Select the service to use, the server's IP address, and the destination interface:

Service: Authentication
Server IP Address:
Destination Interface: LAN

To continue, click Next.

4 Select the type of service for the rule from the **Service** menu. In this example, select **Web** (**HTTP)** to allow network traffic to a Web Server on your LAN.

5 Type the IP address of the mail server in the **IP address** field.

6 Select the destination of the network traffic from the **Destination Interface** menu. In this case, you are sending traffic to the LAN. Select **LAN**.

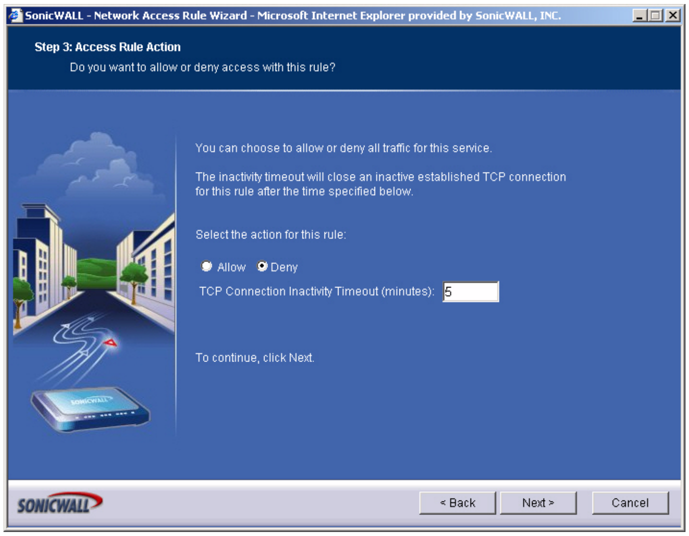
7 Click **Next.** Then click **Apply** to complete the wizard and create a Public Server on your network.

Configuring a General Network Access Rule

1 Click the **Rule Wizard** button at the top right of the **Firewall > Access Rules** page.

2 Select **General Rule**. Click **Next**.

3 You can add an optional text in the **Comment** field. This information is displayed in the Options column of the **Access Rules** table. Click **Next**.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: Access Rule Action

Do you want to allow or deny access with this rule?

You can choose to allow or deny all traffic for this service.

The inactivity timeout will close an inactive established TCP connection for this rule after the time specified below.

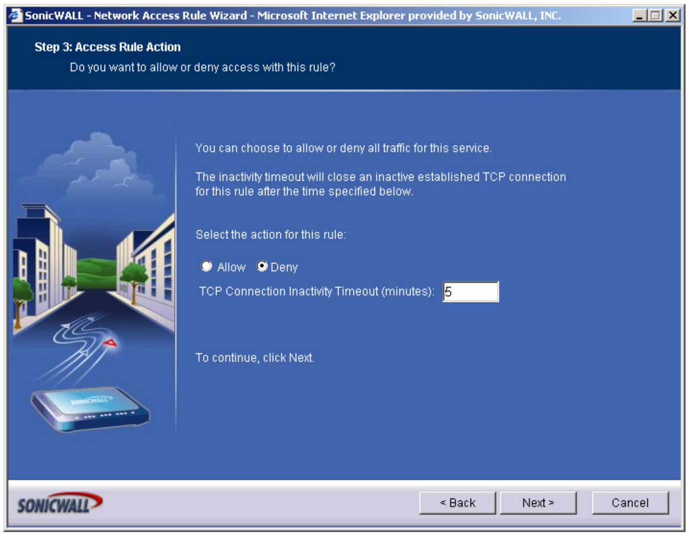
Select the action for this rule:

○ Allow ● Deny
TCP Connection Inactivity Timeout (minutes): 5

To continue, click Next.

4 Select the type of service for the rule. If you do not see the service in the list, you must add it manually to the list of services on the **Firewall > Services** page. Click **Next**.

5 Select **Allow** action to allow the service to the network, or select **Deny** to disallow the service to the network.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: Access Rule Action

Do you want to allow or deny access with this rule?

You can choose to allow or deny all traffic for this service.

The inactivity timeout will close an inactive established TCP connection for this rule after the time specified below.

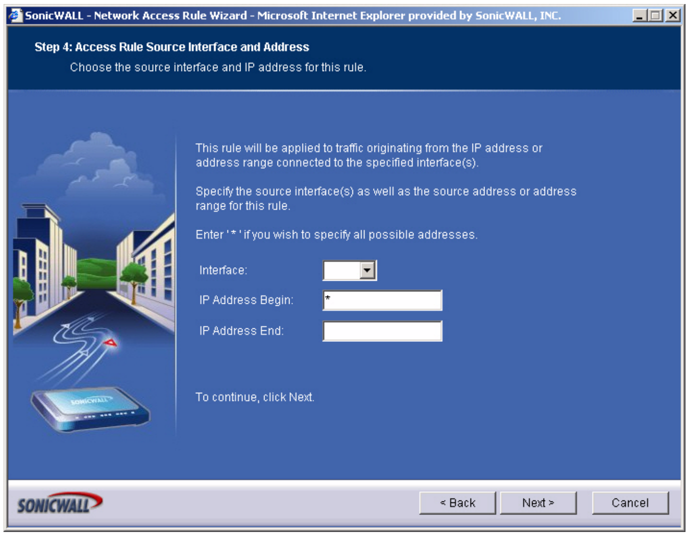
Select the action for this rule:

○ Allow ● Deny

TCP Connection Inactivity Timeout (minutes): 5

To continue, click Next.

6 Enter a value in minutes in the **Inactivity Timeout (minutes)** field. The default value is 5 minutes. Click **Next**.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: Access Rule Source Interface and Address

Choose the source interface and IP address for this rule.

This rule will be applied to traffic originating from the IP address or address range connected to the specified interface(s).

Specify the source interface(s) as well as the source address or address range for this rule.

Enter '*' if you wish to specify all possible addresses.

Interface:

IP Address Begin: *

IP Address End:

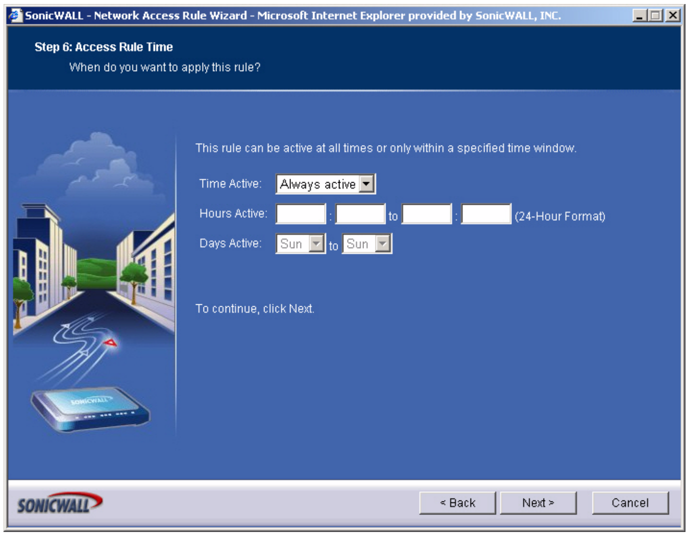
To continue, click Next.

7 Select the source interface of the service from the **Interface** menu. If you want to allow or deny the service from the Internet, select **WAN**. To allow or deny the service from any source, select ***** from the **Interface** menu.

8 If you have a range of IP addresses, enter the first one in the **IP Address Begin** field. If you do not want to specify an IP address, enter “*” in the **IP Address Begin** field. By typing * (asterisk) in the field, all traffic using the service is either allowed or denied to all computers on the network. Click **Next**.

9 Select the destination interface of the service from the **Interface** menu. If you have a range of IP addresses, enter the first one in the **IP Address Begin** field. If you do not want to specify an IP

address, enter “*” in the **IP Address Begin** field. By typing “*****” in the field, all traffic using the service is either allowed or denied to all computers on the network. Click **Next**.


SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Access Rule Time

When do you want to apply this rule?

This rule can be active at all times or only within a specified time window.

Time Active: Always active

Hours Active: : to : (24-Hour Format)

Days Active: Sun to Sun

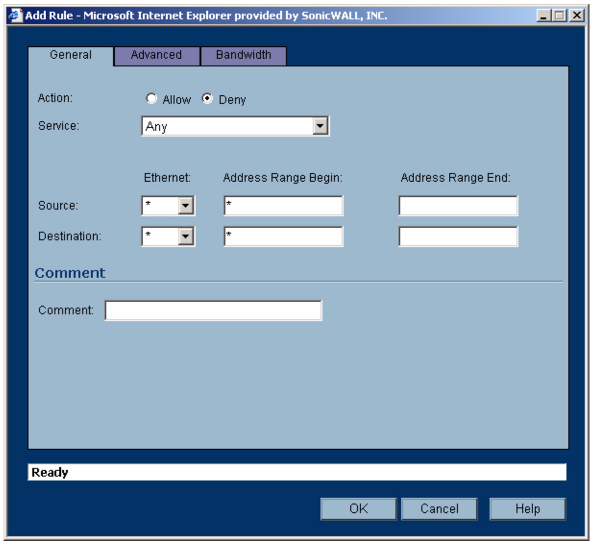
To continue, click Next.

10 The rule is always active unless you specify a time period for the rule to be active. For instance, you can deny access to News (NNTP) between 8 a.m. and 5 p.m. Monday through Friday, but allow access after work hours and on weekends. Specify any specific times in the **Hours Active** fields and the **Days Active** menus. Click **Next.**

11 Click **Apply** to save your new rule. The new rule is listed in the **Access Rules** table.

Adding Rules Using the Add Rule Window

1 Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.


Add Rule - Microsoft Internet Explorer provided by SonicWALL, INC.

Action: ○ Allow ● Deny

Service: Any

	Ethernet:	Address Range Begin:	Address Range End:
Source:	*	*	
Destination:	*	*	

Comment

Comment:

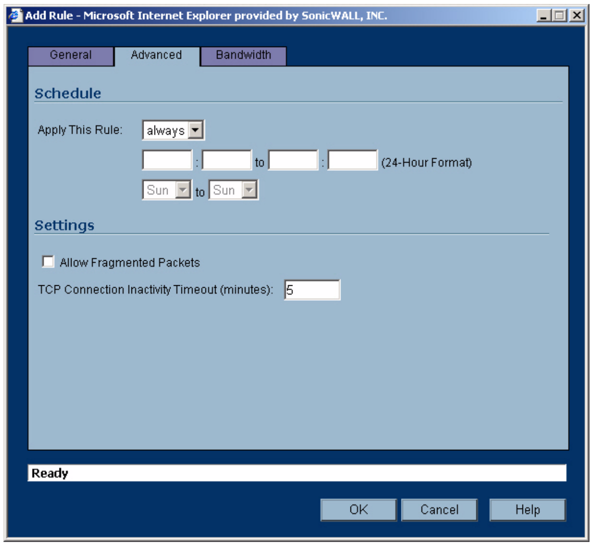
Ready

2 In the **General** page, select **Allow** or **Deny** from the **Action** list depending upon whether the rule is intended to permit or block IP traffic.

3 Select the name of the service affected by the Rule from the **Service** list. If the service is not listed, you must define the service in the **Add Service** window. The **Any** service encompasses all IP services.

4 Select the source of the traffic affected by the rule from the **Source** list.

5. If you want to define the source IP addresses that are affected by the rule, such as restricting certain users from accessing the Internet, enter the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, enter * in the **Address Range Begin** field.
6. Select the destination of the traffic affected by the rule, LAN, WAN, or *, from the **Destination** menu.
7. If you want to define the destination IP addresses that are affected by the rule, for example, to allow inbound Web access to several Web servers on your LAN, enter the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, enter * in the **Address Range Begin** field.
8. Enter any comments to help identify the rule in the **Comments** field.
9. Click the **Advanced** tab.



Apply This Rule: always

☐ Allow Fragmented Packets

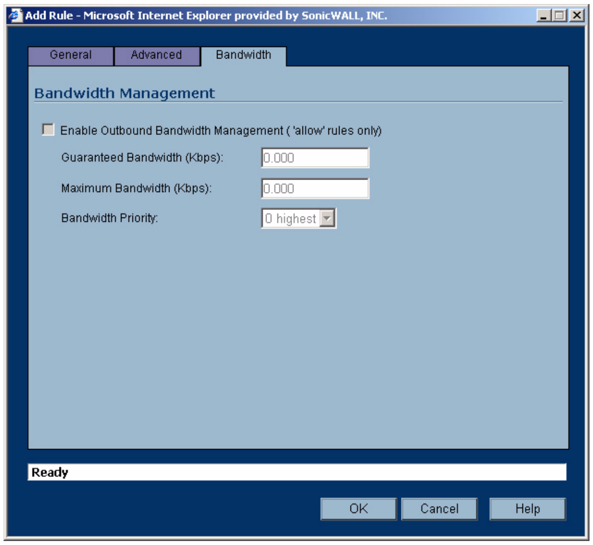
TCP Connection Inactivity Timeout (minutes): 5

10. Select **always** from the **Apply this Rule** menu if the rule is always in effect.
11. Select **from** the **Apply this Rule** menu to define the specific time and day of week to enforce the rule. Enter the time of day (in 24-hour format) to begin and end enforcement. Then select the day of the week to begin and end enforcement.

Tip: *If you want to enable the rule at different times depending on the day of the week, make additional rules for each time period.*

12. If you would like for the rule to time out after a period of inactivity, set the amount of time, in minutes, in the **Inactivity Timeout (minutes)** field. The default value is 5 minutes.
13. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service attacks, the SonicWALL blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPSec.

14 Click the **Bandwidth** tab.


Add Rule - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
Bandwidth
Bandwidth Management
Ready
OK
Cancel
Help

☐ Enable Outbound Bandwidth Management ('allow' rules only)

Guaranteed Bandwidth (Kbps): 0.000

Maximum Bandwidth (Kbps): 0.000

Bandwidth Priority: 0 highest

15 Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

16 Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

✓ **Tip:** *Rules using Bandwidth Management take priority over rules without bandwidth management.*

17 Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list.

18 Click **OK**.

✓ **Tip:** *Although custom rules can be created that allow inbound IP traffic, the SonicWALL does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.*

Rule Examples

The following examples illustrate methods for creating Network Access Rules.

Blocking LAN Access for Specific Services

This example shows how to block LAN access to NNTP servers on the Internet during business hours.

1. Click **Add** to launch the **Add** window.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** window.
4. Select **LAN** from the **Source Ethernet** menu.
5. Since all computers on the LAN are to be affected, enter * in the **Source Address Range Begin** field.
6. Select **WAN** from the **Destination Ethernet** menu.
7. Enter * in the **Destination Address Range Begin** field to block access to all NNTP servers.
8. Click on the **Options** tab.
9. Select **from** the **Apply this Rule** list to configure the time of enforcement.
10. Enter 8:30 and 17:30 in the hour fields.
11. Select **Mon** to **Fri** from the menu.
12. Click **OK**.

Enabling Ping

By default, your SonicWALL does not respond to ping requests from the Internet. This Rule allows ping requests from your ISP servers to your SonicWALL security appliance.

1. Click **Add** to launch the **Add Rule** window.
2. Select **Allow** from the **Action** menu.
3. Select **Ping** from the **Service** menu.
4. Select **WAN** from the **Source Ethernet** menu.
5. Enter the starting IP address of the ISP network in the **Source Address Range Begin** field and the ending IP address of the ISP network in the **Source Address Range End** field.
6. Select **LAN** from the **Destination Ethernet** menu.
7. Since the intent is to allow a ping only to the SonicWALL security appliance, enter the SonicWALL security appliance LAN IP Address in the **Destination Address Range Begin** field.
8. Click the **Options** tab.
9. Select **Always** from the **Apply this Rule** menu to ensure continuous enforcement.
10. Click **OK**.

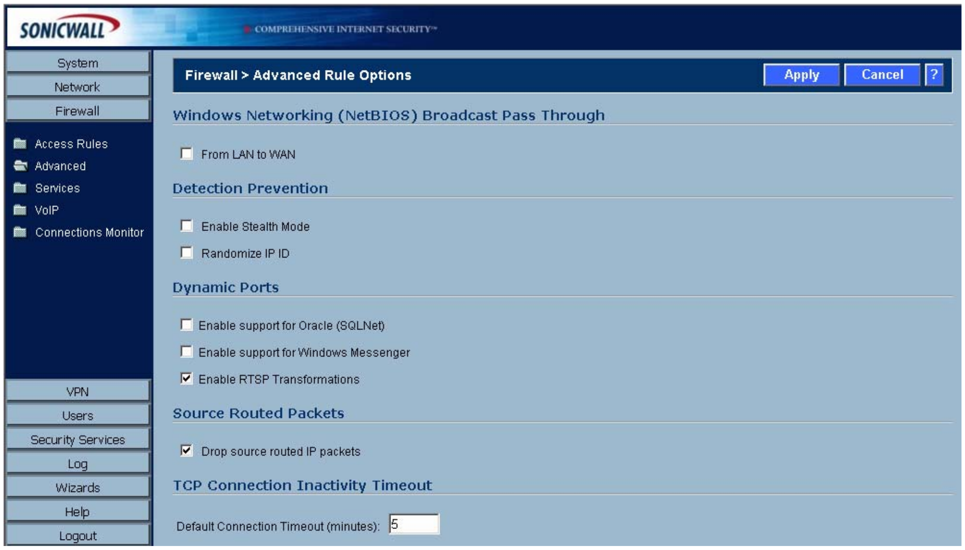
CHAPTER

32

Configuring Advanced Rule Options

Access Rules > Advanced

Click **Advanced** underneath Access Rules.The **Advanced Rule Options** page is displayed.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
Access Rules
Advanced
Services
VoIP
Connections Monitor
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?

Firewall > Advanced Rule Options

Windows Networking (NetBIOS) Broadcast Pass Through

☐ From LAN to WAN

Detection Prevention

☐ Enable Stealth Mode
☐ Randomize IP ID

Dynamic Ports

☐ Enable support for Oracle (SQLNet)
☐ Enable support for Windows Messenger
☑ Enable RTSP Transformations

Source Routed Packets

☑ Drop source routed IP packets

TCP Connection Inactivity Timeout

Default Connection Timeout (minutes): 5

Windows Networking (NetBIOS) Broadcast Pass Through

Computers running Microsoft Windows communicate with one another through NetBIOS broadcast packets. By default, the SonicWALL security appliance blocks these broadcasts. You can choose the interfaces you want to allow Windows networking broadcast pass-through for supporting Windows networking.

Detection Prevention

Enable Stealth Mode

By default, the SonicWALL security appliance responds to incoming connection requests as either “blocked” or “open”. If you enable **Stealth Mode**, your SonicWALL security appliance does not respond to blocked inbound connection requests. **Stealth Mode** makes your SonicWALL security appliance essentially invisible to hackers.

Randomize IP ID

Select **Randomize IP ID** to prevent hackers using various detection tools from detecting the presence of a SonicWALL security appliance. IP packets are given random IP IDs which makes it more difficult for hackers to “fingerprint” the SonicWALL security appliance.

Dynamic Ports

- Select **Enable support for Oracle (SQLNet)** if you have Oracle applications on your network.
- Select **Enable Support for Windows Messenger** if you are having problems using Windows Messenger and Windows XP through the SonicWALL security appliance. If **Enable Support for Windows Messenger** is selected, it may affect the performance of the SonicWALL security appliance.
- Select **Enable RTSP Transformations** to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

Drop Source Routed Packets is selected by default. Clear the check box if you are testing traffic between two specific hosts and you are using source routing.

TCP Connection Inactivity Timeout

If a connection to a remote server remains idle for more than five minutes, the SonicWALL security appliance closes the connection. Without this timeout, Internet connections could stay open indefinitely, creating potential security holes. You can increase the **Inactivity Timeout** if applications, such as Telnet and FTP, are frequently disconnected.

TCP Checksum Validation

Enable TCP checksum validation - enables TCP checksum validation for error checking.

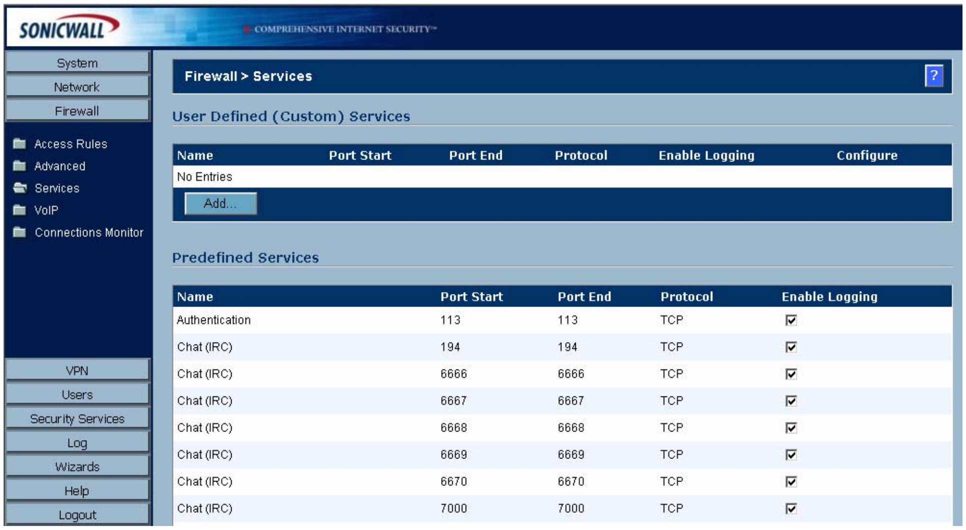
Access Rule Service Options

Force inbound and outbound FTP data connections to use default port: 20 - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

CHAPTER 33

Configuring Custom Services

Firewall > Services


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
Access Rules
Advanced
Services
VoIP
Connections Monitor
VPN
Users
Security Services
Log
Wizards
Help
Logout
Firewall > Services
?
Add...

User Defined (Custom) Services

Name	Port Start	Port End	Protocol	Enable Logging	Configure
No Entries					

Predefined Services

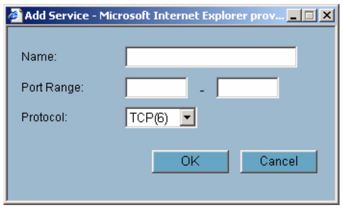
Name	Port Start	Port End	Protocol	Enable Logging
Authentication	113	113	TCP	☑
Chat (IRC)	194	194	TCP	☑
Chat (IRC)	6666	6666	TCP	☑
Chat (IRC)	6667	6667	TCP	☑
Chat (IRC)	6668	6668	TCP	☑
Chat (IRC)	6669	6669	TCP	☑
Chat (IRC)	6670	6670	TCP	☑
Chat (IRC)	7000	7000	TCP	☑

Services are anything a server provides to other computers. A service can be as simple as the computer asking a server for the correct time (NTP) and the server returns a response. Other types of services provide access to different types of data. Web servers (HTTP) respond to requests from clients (browser software) for access to files and data. Services are used by the SonicWALL security appliance to configure network access rules for allowing or denying traffic to the network.

User Defined (Custom) Services

If protocol is not listed in the **Predefined Services** table, you can add it to the User Defined (Custom) Services table.

1 Click **Add**. **The Add Service** window is displayed.



Name:
Port Range: -
Protocol: TCP(6)

2 Enter the name of the service in the **Name** field.

3 Enter the port number or numbers that apply to the service in the **Port Range** fields. A list of well know port numbers can be found in any networking reference.

4 Select the type of protocol, **TCP**, **UDP**, or **ICMP** from the **Protocol** menu.

5 Click **OK**. The service appears in the **User Defined (Custom) Services** table.

Predefined Services

The **Predefined Services** table lists are the services that are predefined in the SonicWALL security appliance. You cannot delete any of these predefined services.

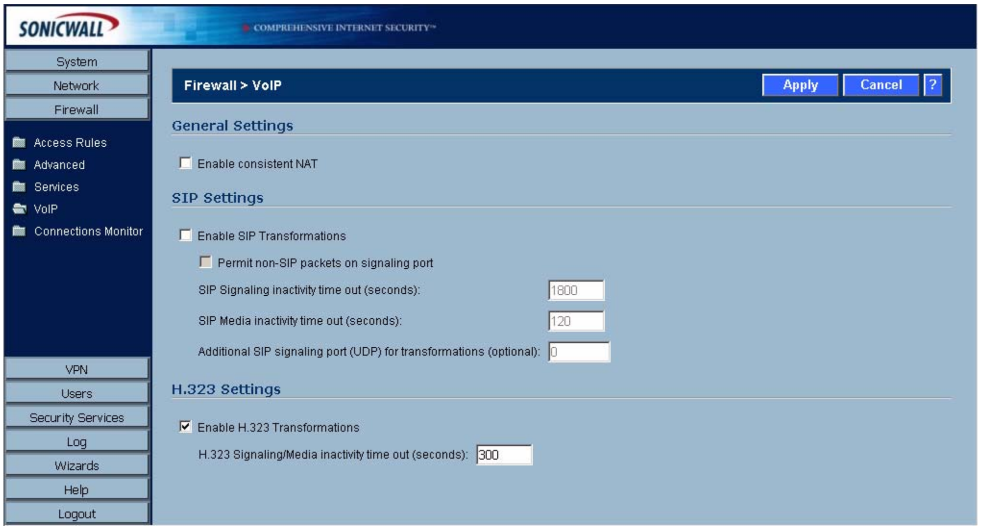
The Predefined Services table displays the following information about each predefined service:

- **Name** - the name of the service
- **Port Start** - the beginning port number associated with the service
- **Port End** - the ending port number associated with the service
- **Protocol** - the protocol the service is associated with: TCP, UDP, ICMP or IPSEC-ESP
- **Enable Logging** - checked, the service traffic is logged by the SonicWALL security appliance event log. Unchecked, the service traffic is not logged.

CHAPTER 34

Configuring VoIP

Firewall > VoIP


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
Access Rules
Advanced
Services
VoIP
Connections Monitor
VPN
Users
Security Services
Log
Wizards
Help
Logout
Firewall > VoIP
Apply
Cancel
?

General Settings

☐ Enable consistent NAT

SIP Settings

☐ Enable SIP Transformations

☐ Permit non-SIP packets on signaling port

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

Additional SIP signaling port (UDP) for transformations (optional): 0

H.323 Settings

☑ Enable H.323 Transformations

H.323 Signaling/Media inactivity time out (seconds): 300

The SonicWALL security appliance supports the most widely used VoIP standard protocols and the most commonly used VoIP vendors and systems on the market. Providing full VoIP support on the SonicWALL security appliance enables organizations with increasingly decentralized workforces to access corporate voice services from remote sites. VoIP systems consist of multiple clients (such as IP phones or soft phones) and VoIP servers residing at different parts of the network.

VoIP Protocols

VoIP (Voice over IP) is a term used in IP telephony for a set of facilities for managing the delivery of voice information using IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by traditional telephone service.

This section provides a concept overview on H.323 and SIP protocols. Refer to the “Configuring the VoIP Settings” section for configuration tasks for H.323 and SIP networks.

H.323

H.323 is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet.

H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC
- **Gateways** - Connectivity between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN)
- **Gatekeepers** - Services for call setup and tear down, and registering H.323 terminals for communications
- **Multipoint control units (MCUs)** - Three-way and higher multipoint communications between terminals

SIP

Session Initiation Protocol (SIP) is a signaling protocol used in VoIP. Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

Configuring the VoIP Settings

The SonicWALL security appliance allows VoIP phone and applications to be deployed behind the firewall. The **Firewall > VoIP** page includes the settings for supporting VoIP traffic on the SonicWALL security appliance.

SIP Settings

This section provides configuration tasks for **SIP Settings**.

- **Enable SIP Transformations -** This setting transforms SIP messages between LAN (trusted) and WAN (untrusted). You need to check this setting when you want the SonicWALL to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select Enable SIP Transformations to transform the SIP messages. It's recommended that you turn on **Enable SIP Transformations** unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode and it transforms messages going from LAN to WAN and vice versa.
- **Permit non-SIP packets on signalling port** - This checkbox is disabled by default. Select this checkbox for enabling applications such as Apple iChat. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic.
- **SIP Signalling inactivity time out (seconds)** - This field has a default value of 1200 seconds (20 minutes).
- **SIP Media inactivity time out (seconds)** - This field has a default value of 120 seconds (2 minutes).

H.323 Settings

This section provides configuration tasks for H.323 Settings.

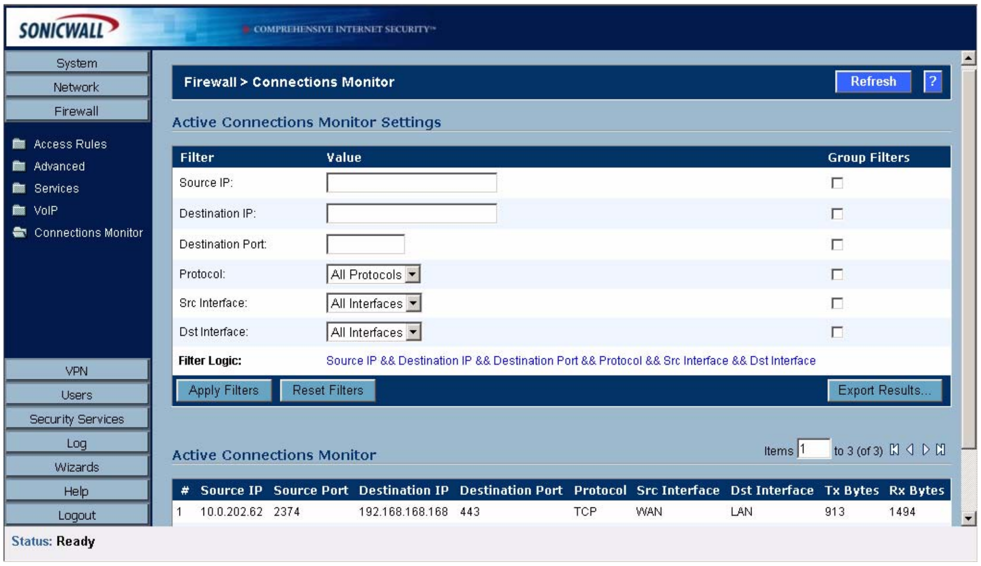
- **Enable H.323 Transformation** - Select this option to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL. The SonicWALL performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Clear the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL.
- **H.323 Signalling/Media inactivity time out (seconds)** - This field has a default value of 300 seconds (5 minutes). This is a similar setting to the “TCP connection inactivity timeout.”

CHAPTER 35

Monitoring Active Firewall Connections

Firewall > Connections Monitor

The **Firewall > Connections Monitor** page provides you the filtering controls to query log event messages based on your configured filter logic.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
Access Rules
Advanced
Services
VoIP
Connections Monitor
VPN
Users
Security Services
Log
Wizards
Help
Logout
Firewall > Connections Monitor
Refresh
?
Apply Filters
Reset Filters
Export Results...
Items
Status: Ready

Active Connections Monitor Settings

Filter	Value	Group Filters
Source IP:		☐
Destination IP:		☐
Destination Port:		☐
Protocol:	All Protocols	☐
Src Interface:	All Interfaces	☐
Dst Interface:	All Interfaces	☐
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface	

Active Connections Monitor

Items 1 to 3 (of 3)

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.62	2374	192.168.168.168	443	TCP	WAN	LAN	913	1494

Setting Filter Logic

By default, the SonicOS filter logic is set to “Priority && Category && Source && Destination.” The double ampersand symbols (&&) indicate the boolean expression “and.” The default SonicOS filter logic displays all log events.

1. Enter the source IP address in the **Source IP** field.
2. Enter the destination IP address in the **Destination IP** field.
3. Enter the destination port number in the **Destination Port** field.
4. Select the protocol from the **Protocol** menu.
5. Select the source interface from the **Src Interface**.
6. Select the destination interface from **Dst Interface**.
7. Click **Apply Filters**.

Using Group Filters

Use **Group Filters** to change the default SonicOS filter logic (Priority && Category && Source && Destination) from double ampersand symbols (&&) to double pipe symbols (||) to indicate the boolean expression “or.” When using group filters, select two or more **Group Filters** checkboxes.

If you select only one **Group Filter** checkbox, the filter logic will remain the same. Selecting only the Priority-Group Filter checkbox provides you with the following filter logic:

Source IP: (Priority) && Category && Source && Destination

PART 8

VPN

CHAPTER 36

Configuring VPN Settings

SonicWALL VPN Options Overview

The SonicWALL security appliance can be configured to support remote VPN clients and/or site-to-site VPN connections between offices. SonicWALL VPN is based on the industry-standard IPSec VPN implementation.

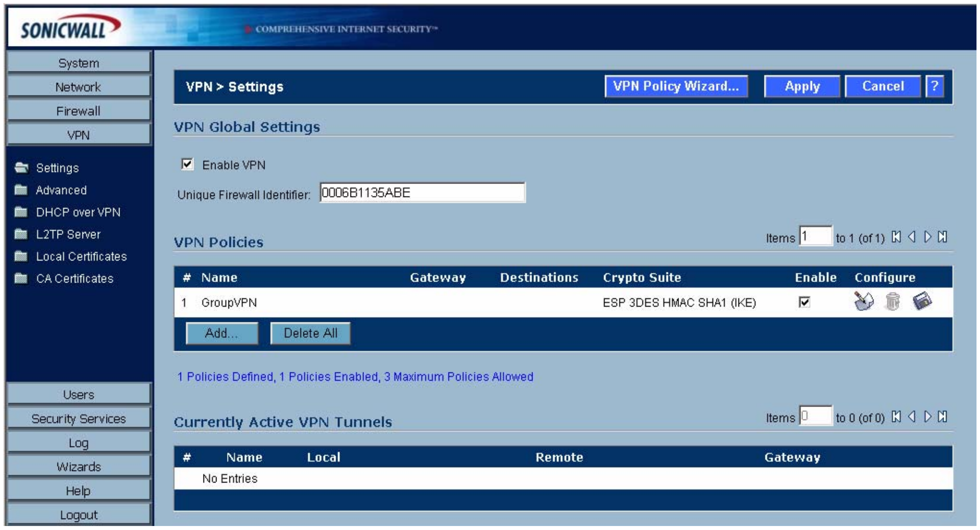
Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client or Global Security Client and SonicWALL GroupVPN on your SonicWALL security appliance.

Note: *For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**. Both guides on the SonicWALL security appliance Resource CD or available at the SonicWALL documentation Web site at <http://www.sonciwall.com/services/documentation.html>*

Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections. Using the SonicWALL security appliance's management interface, you can quickly create a VPN policy to a remote site. Whenever data is intended for the remote site, the SonicWALL automatically encrypts the data and sends it over the Internet to the remote site, where it is decrypted and forwarded to the intended destination.

VPN > Settings

The **VPN > Settings** page provides the SonicWALL features for configuring site-to-site VPN connections and client VPN connections.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
VPN > Settings
VPN Policy Wizard...
Apply
Cancel
?
Add...
Delete All

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B1135ABE

VPN Policies

Items 1 to 1 (of 1)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☑	

1 Policies Defined, 1 Policies Enabled, 3 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 0 to 0 (of 0)

#	Name	Local	Remote	Gateway
	No Entries			

The **GroupVPN** policy is automatically enabled and ready to use for supporting remote SonicWALL Global VPN Clients.

VPN Global Settings

The **Global VPN Settings** section displays the following information:

- **Enable VPN** must be selected to allow VPN policies through the SonicWALL.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

- **Name** - user-defined name to identify the Security Association.
- **Gateway** - the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations** - the IP addresses of the destination networks.
- **Crypto Suite** - the type of encryption used
- **Enable** - selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure** - edit or delete the VPN Policy information. GroupVPN has a **Disk** icon for exporting the configuration for SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table.

Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column header indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the Peer Gateway IP address.

Configuring GroupVPN Policy on the SonicWALL

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple VPN clients by the administrator of the SonicWALL security appliance. **GroupVPN** allows for easy deployment of multiple SonicWALL Global VPN Clients or Global Security Clients.

Note: *For more information on the SonicWALL Global Security Client, refer to the SonicWALL Global Security Client Administrator’s Guide on the Resource CD or available on the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html>.*

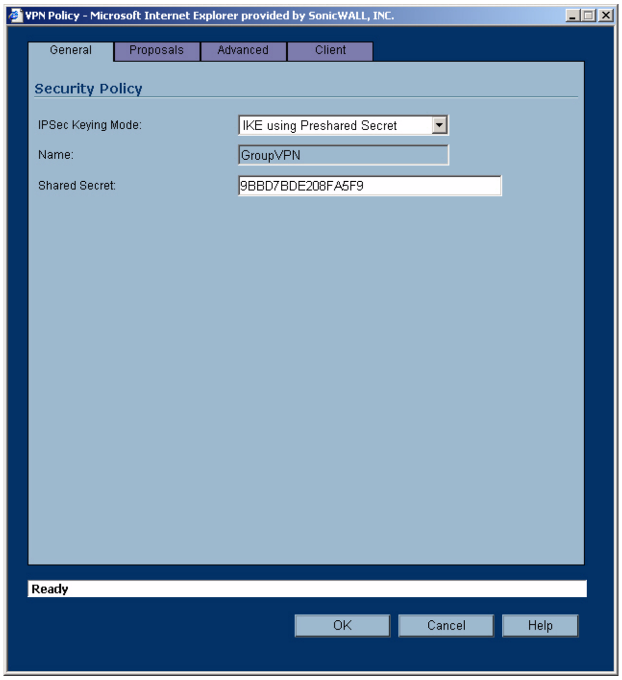
The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients using **IKE using Preshared Secret** without any further editing of the VPN policy. You can configure GroupVPN to use **IKE using 3rd Party Certificates** as your IPSec Keying Mode instead of **IKE using Preshared Secret**.

To enable GroupVPN using the default **IKE using Preshared Secret** settings, simply click the **Enable** checkbox in the **VPN Policies** table.

Configuring IKE Preshared Secret

To edit the default settings for GroupVPN, follow these steps:

1 Click the edit icon in the **GroupVPN** entry. The **VPN Policy** window is displayed.

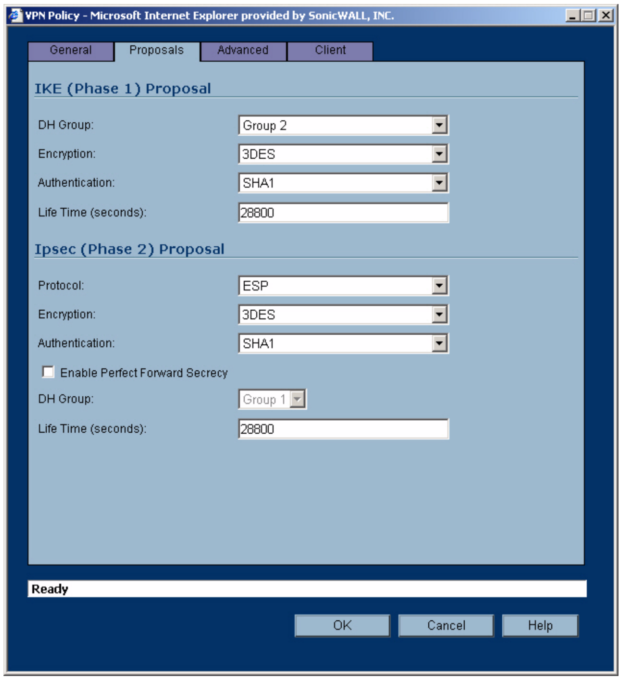

VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret
Name: GroupVPN
Shared Secret: 9BBD7BDE208FA5F9

2 In the **General** tab, **IKE using Preshared Secret** is the default setting for **IPSec Keying Mode**. A Shared Secret is automatically generated in the **Shared Secret** field, or you can generate your own shared secret. Shared Secrets must be minimum of four characters.

3 Click the **Proposals** tab to continue the configuration process.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

IKE (Phase 1) Proposal

DH Group: Group 2
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP
Encryption: 3DES
Authentication: SHA1
☐ Enable Perfect Forward Secrecy
DH Group: Group 1
Life Time (seconds): 28800

In the **IKE (Phase 1) Proposal** section, select the following settings:

Group 2 from the **DH Group** menu.

3DES from the **Encryption** menu

SHA1 from the **Authentication** menu

Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

In the **IPSec (Phase 2) Proposal** section, select the following settings:

ESP from the **Protocol** menu

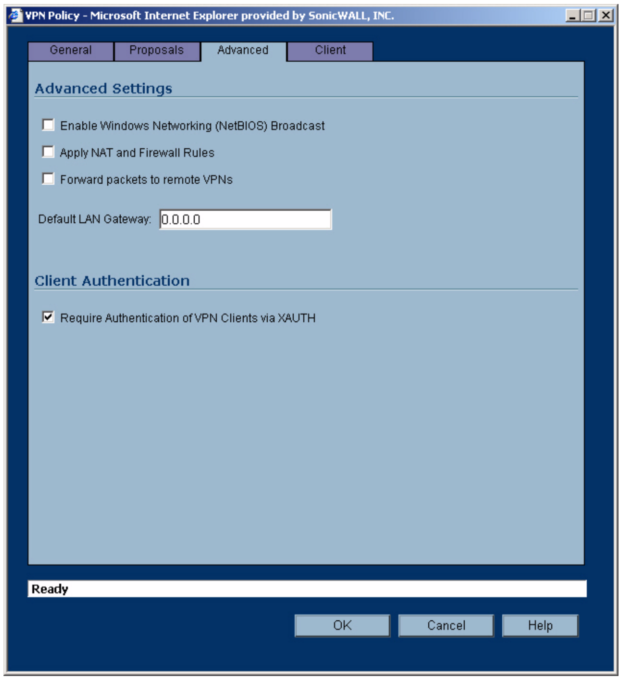
3DES from the **Encryption** menu

MD5 from the **Authentication** menu

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Then select Group 2 from the **DH Group** menu.

Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

4 Click the **Advanced** tab. Select any of the following settings you want to apply to your GroupVPN policy.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

Advanced Settings

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Apply NAT and Firewall Rules

☐ Forward packets to remote VPNs

Default LAN Gateway: 0.0.0.0

Client Authentication

☑ Require Authentication of VPN Clients via XAUTH

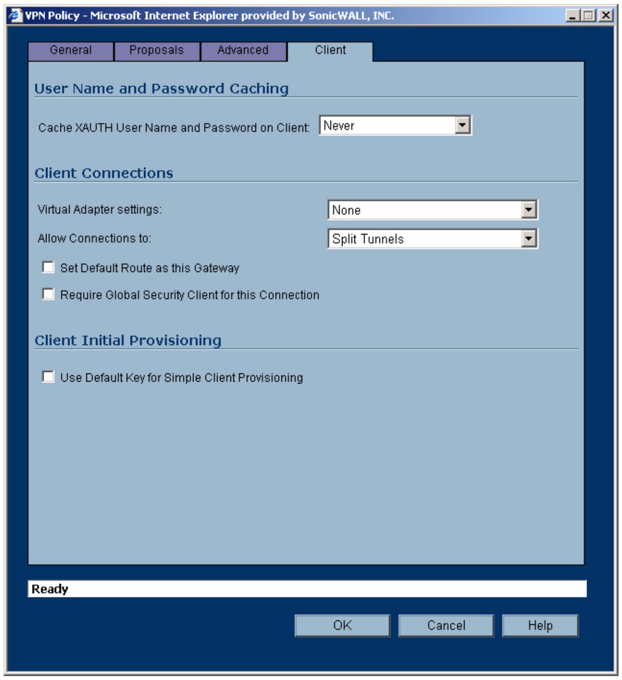
Ready

- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site’s LAN subnet to be hidden from the corporate site, and is most useful when a remote office’s network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.

▲ **Alert:** *Offices can have overlapping LAN IP ranges if the* ***Apply NAT and Firewall Rules*** *feature is selected.*

- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the **Routing** page located in the **Network** section. Enabling this feature allows a network administrator to create a “hub and spoke” network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a “hub and spoke” network, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using **Use this VPN Tunnel as default route for all Internet traffic**. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ/WLAN, or LAN/OPT/DMZ/WLAN** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ/WLAN network.
- **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

5 Click the **Client** tab. Select any of the following settings you want to apply to your GroupVPN policy.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

☐ Set Default Route as this Gateway

☐ Require Global Security Client for this Connection

Client Initial Provisioning

☐ Use Default Key for Simple Client Provisioning

Ready

Cache XAUTH User Name and Password - Allows Global VPN Client to cache any username and password required for XAUTH user authentication. The drop-down list provides the following options:

- **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.

- **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
- **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

Virtual Adapter Settings - The use of the Virtual Adapter by the Global VPN Client (GVC) has always been dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it was necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.

- **None** - A Virtual Adapter will not be used by this GroupVPN connection.
- **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
- **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. **Note:** By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

Allow Connections to - Specifies single or multiple VPN connections. The drop-down list provides the following options:

- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of this gateway is sent through the VPN tunnel. All other traffic is blocked. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with Set Default Route as this Gateway, then Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked. Only one of the multiple gateways can have Set Default Route as this Gateway enabled.
- **Split Tunnels** - Allows the VPN user to have both local Internet access and VPN connectivity.

Set Default Route as this Gateway - If checked, Global VPN Client traffic that does not match selectors for the gateway’s protected subnets must also be tunnelled. In effect, this changes the Global VPN Client’s default gateway to the gateway tunnel endpoint. If unchecked, the Global VPN Client must drop all non-matching traffic if Allow traffic to This Gateway Only or All Secured Gateways is selected.

Require Global Security Client for this Connection - Allows a VPN connection from the remote Global Security Client only if the remote computer is running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection.

Use Default Key for Simple Client Provisioning - If set, authentication of initial Aggressive mode exchange uses a default Preshared Key by gateway and all Global VPN Clients. This allows for the control of the use of the default registration key. If not set, then Preshared Key must be distributed out of band.

6. Click **OK**.

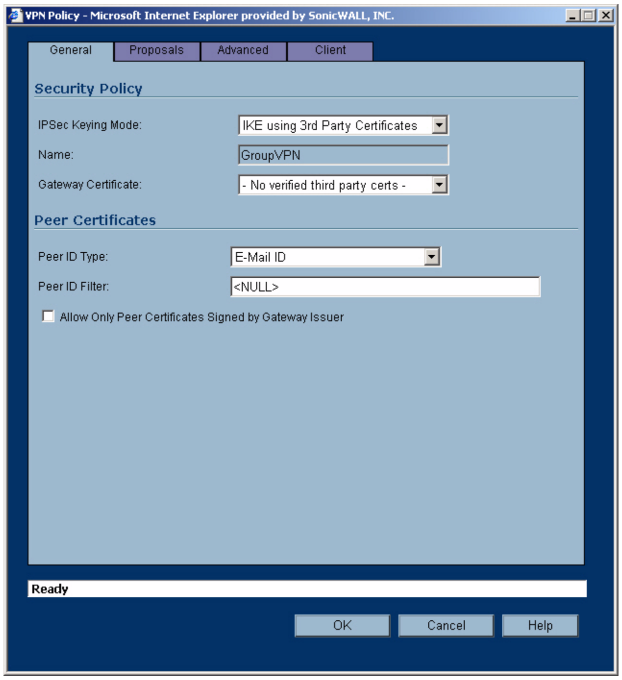
Configuring GroupVPN with IKE 3rd Party Certificates

To configure your GroupVPN policy with IKE 3rd Party Certificates, follow these steps:

Alert: *Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWALL.*

1 In the **VPN > Settings** page click the edit icon under **Configure** for the **GroupVPN** entry. The **VPN Policy** window is displayed.

2 In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **IPSec Keying Mode** menu. The SA name is **Group VPN** by default and cannot be changed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using 3rd Party Certificates

Name: GroupVPN

Gateway Certificate: - No verified third party certs -

Peer Certificates

Peer ID Type: E-Mail ID

Peer ID Filter: <NULL>

☐ Allow Only Peer Certificates Signed by Gateway Issuer

Ready

3 Select a certificate for the SonicWALL from the **Gateway Certificate** menu.

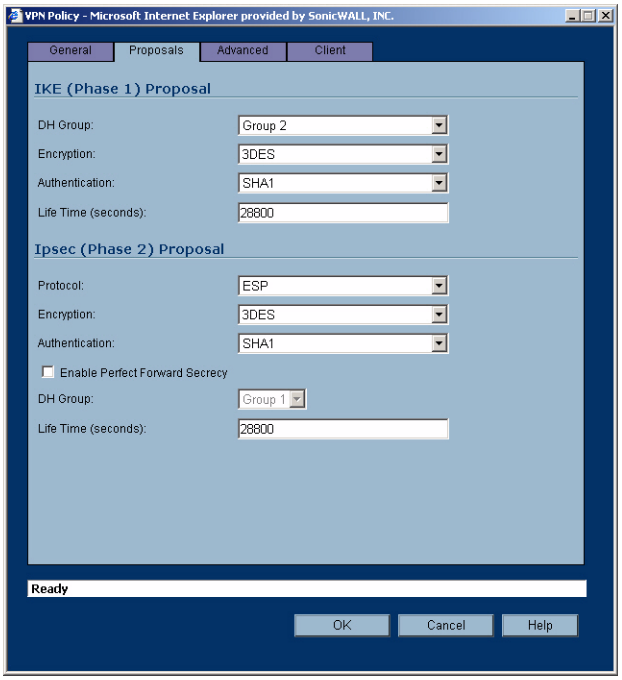
4 Select one of the following Peer ID types from the **Peer ID Type** menu and enter the Peer ID filter information in the **Peer ID Filter** field.

E-Mail ID and Domain Name - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The certificate verification process did not actually verify my email address or domain name, just that the certificate I selected to use, had this matching entry contained in the Alternative Subject Name field. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

Distinguished Name - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). Up to three organizational units can be specified. The usage is c=*;o=*;ou=*;ou=*;ou=*;cn=*. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. c=us.

5 Check **All Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the Gateway Certificate menu.

6 Click on the **Proposals** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

IKE (Phase 1) Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

DH Group: Group 1

Life Time (seconds): 28800

7 In the **IKE (Phase 1) Proposal** section, select the following settings:

Group 2 from the **DH Group** menu.

3DES from the **Encryption** menu.

SHA1 from the **Authentication** menu.

Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

8 In the **IPSec (Phase 2) Proposal** section, select the following settings:

ESP from the **Protocol** menu.

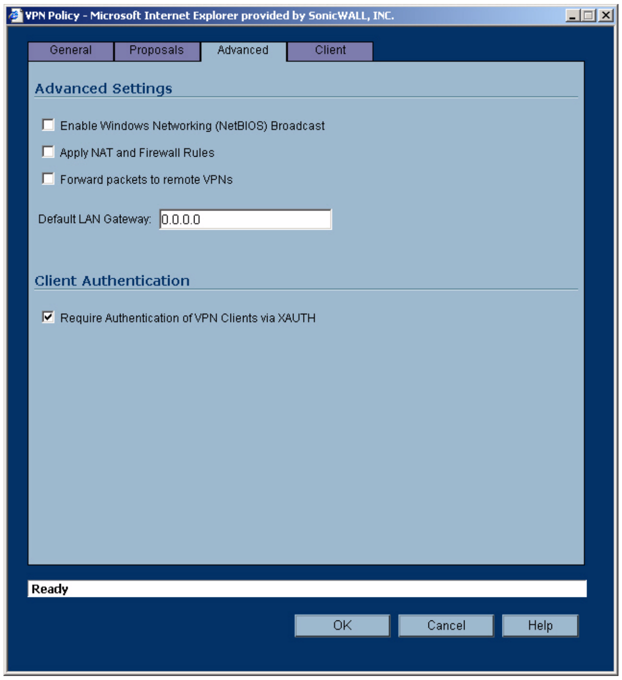
3DES from the **Encryption** menu.

MD5 from the **Authentication** menu.

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Then select **Group 2** from the **DH Group** menu.

Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

9 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN policy:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

Advanced Settings

☐ Enable Windows Networking (NetBIOS) Broadcast
☐ Apply NAT and Firewall Rules
☐ Forward packets to remote VPNs

Default LAN Gateway: 0.0.0.0

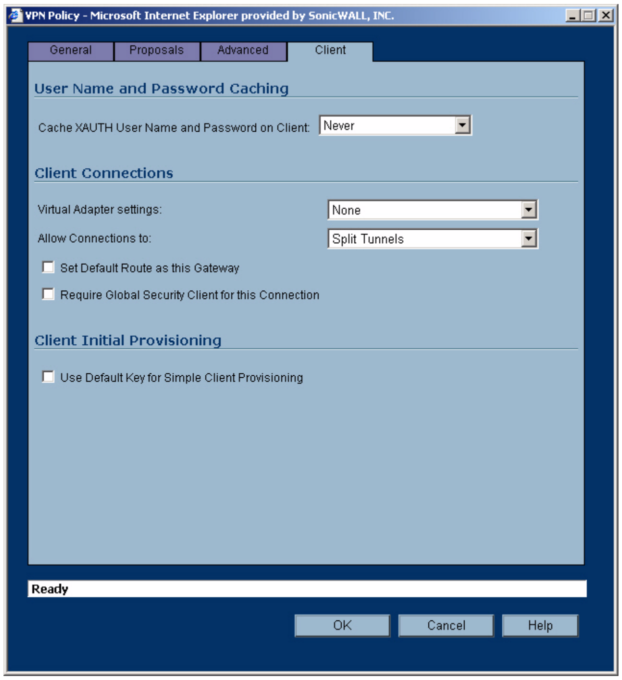
Client Authentication

☑ Require Authentication of VPN Clients via XAUTH

- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN. If the SonicWALL uses the Transparent Mode network configuration, using this check box applies the firewall access rules and checks for attacks, but not does not apply NAT.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the Routing page located in the Network section. Enabling this feature allows a network administrator to create a "hub and spoke" network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a "hub and spoke" network, select the Forward Packets to Remote VPNs check box. Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all Internet traffic through this SA check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **VPN Terminated at the LAN, OPT/DMZ/WLAN, or LAN/OPT/DMZ/WLAN** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ/WLAN network.
- **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

10 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

☐ Set Default Route as this Gateway

☐ Require Global Security Client for this Connection

Client Initial Provisioning

☐ Use Default Key for Simple Client Provisioning

Ready

Cache XAUTH User Name and Password - Allows Global VPN Client to cache any username and password required for XAUTH user authentication. The drop-down list provides the following options:

- **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
- **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
- **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

Virtual Adapter Settings - The use of the Virtual Adapter by the Global VPN Client (GVC) has always been dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it was necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation.

To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.

- **None** - A Virtual Adapter will not be used by this GroupVPN connection.
- **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.

- **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. **Note:** By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

Allow Connections to - Specifies single or multiple VPN connections. The drop-down list provides the following options:

- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of this gateway is sent through the VPN tunnel. All other traffic is blocked. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with Set Default Route as this Gateway, then Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked. Only one of the multiple gateways can have Set Default Route as this Gateway enabled.
- **Split Tunnels** - Allows the VPN user to have both local Internet access and VPN connectivity.

Set Default Route as this Gateway - If checked, Global VPN Client traffic that does not match selectors for the gateway's protected subnets must also be tunnelled. In effect, this changes the Global VPN Client's default gateway to the gateway tunnel endpoint. If unchecked, the Global VPN Client must drop all non-matching traffic if Allow traffic to This Gateway Only or All Secured Gateways is selected.

Require Global Security Client for this Connection - Allows a VPN connection from the remote Global Security Client only if the remote computer is running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection.

Use Default Key for Simple Client Provisioning - If set, authentication of initial Aggressive mode exchange uses a default Preshared Key by gateway and all Global VPN Clients. This allows for the control of the use of the default registration key. If not set, then Preshared Key must be distributed out of band.

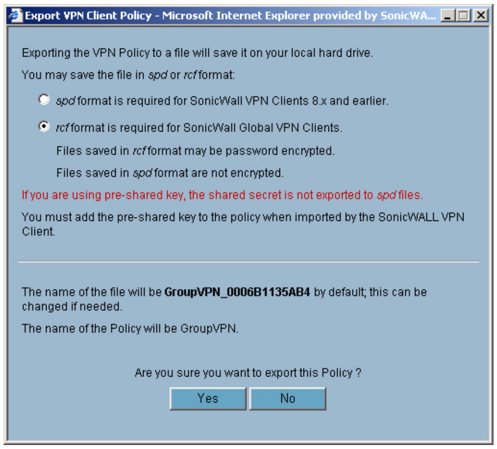
13. Click **OK**. Then click **Apply** to enable the changes.

Export a GroupVPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

▲ **Alert:** *The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.*

1 Click the **Disk** icon under **Configure** for the **GroupVPN** policy. The **Export VPN Client Policy** window is displayed.


Export VPN Client Policy - Microsoft Internet Explorer provided by SonicWA...

Exporting the VPN Policy to a file will save it on your local hard drive.

You may save the file in *spd* or *rcf* format:

○ *spd* format is required for SonicWall VPN Clients 8.x and earlier.

● *rcf* format is required for SonicWall Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWALL VPN Client.

The name of the file will be **GroupVPN_0006B1135AB4** by default; this can be changed if needed.

The name of the Policy will be GroupVPN.

Are you sure you want to export this Policy ?

2 **rcf format is required for SonicWALL Global Clients** is selected by default. Files saved in the rcf format can be password encrypted.

3 Click **Yes**. The **VPN Policy Export** window is displayed.

4 If you want to encrypt the exported file, type a password in the **Password** field, re-enter the password in the **Confirm Password** field, and then click **Submit**.

5 If you do not want the exported file encrypted, click Submit. A message appears confirming your choice. Click **OK**.

6 Select the locations to save the file and click **Save**.

7 Click **Close**. The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Site to Site VPN Configurations

You can configure the SonicWALL security appliance for site-to-site VPN connections using the **VPN Policy Wizard** or the **VPN Policy** window.

Site-to-Site VPN Deployments

When designing VPN connections, be sure to document all pertinent IP Addressing information and create a network diagram to use as a reference. A sample planning sheet is provided. The SonicWALL must have a routable WAN IP Address whether it is dynamic or static. Be sure that the networks behind the SonicWALLs are unique. The same subnets cannot reside behind two different VPN gateways.

In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site to Site VPN Configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPSec to another manufacturer’s firewall.
- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWALL.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

VPN Planning Sheet for Site-to-Site VPN Policies

You need the information below before you begin configuring Site-to-Site VPN Policies.

Site A

Workstation

LAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

SonicWALL

LAN IP Address: ___.___.___.___

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

Router

Internet Gateway

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

DNS Server #1: ___.___.___.___

DNS Server #2: ___.___.___.___

Additional Information

SA Name:____________________

Manual Key, SPI In_____ SPI Out_____

Enc.Key:____________________

Auth.Key:___________________

If Preshared Secret,

Shared Secret:___________________

Phase 1 DH - 1 2 5

SA Lifetime 28800 or ____________

Phase 1 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

Phase 2 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

ARC NULL

Configuring Site to Site VPN Policies Using the VPN Policy Wizard

The **VPN Policy Wizard** quickly and easily walks you through the steps of configuring a VPN security policy between two SonicWALL appliances.

The **VPN Policy Wizard** allows you to create a **Typical** VPN connection. Using this option, the wizard creates a VPN policy based on **IKE using Preshared Secret**.

Using the **Custom** option in the **VPN Policy Wizard** allow you to create a VPN policy with your own configuration options based on one of the following IPSec Keying Modes:

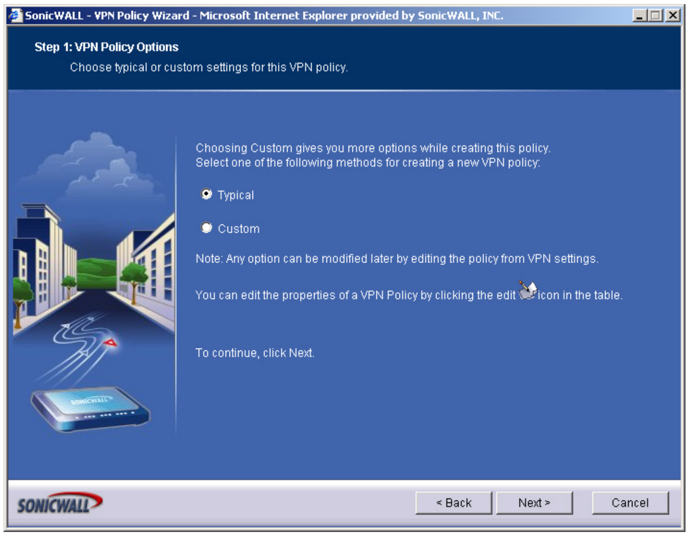
- IKE using Preshared Secret
- Manual Key
- IKE using 3rd Party Certificates

Note: *You need IP addressing information for your local network as well as your remote network. Use the VPN Planning Sheet to record your information.*

Creating a Typical IKE Preshared Secret VPN Policy

You can create a **Typical** VPN policy using the **VPN Policy Wizard** to configure an IPSec VPN security association between two SonicWALL appliances.

1 Click **VPN Policy Wizard** on the **VPN > Settings** page to launch the wizard. Click **Next**.



SonicWALL - VPN Policy Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: VPN Policy Options

Choose typical or custom settings for this VPN policy.

Choosing Custom gives you more options while creating this policy.
Select one of the following methods for creating a new VPN policy:

● Typical

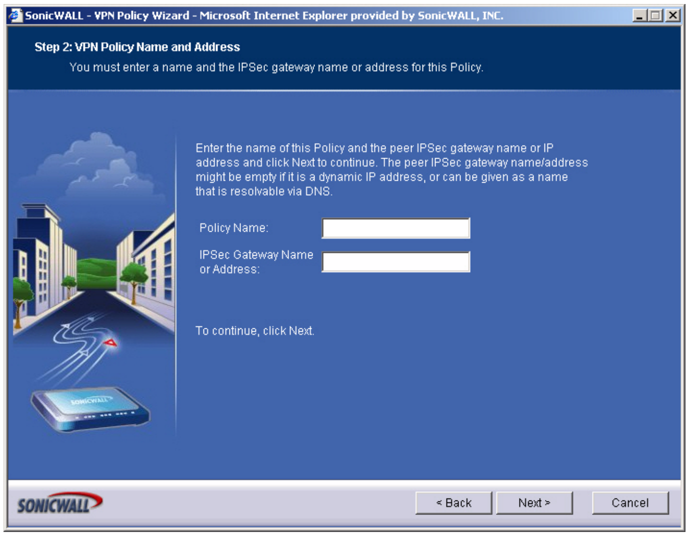
○ Custom

Note: Any option can be modified later by editing the policy from VPN settings.

You can edit the properties of a VPN Policy by clicking the edit icon in the table.

To continue, click Next.

2 Select **Typical** and click **Next.**



SonicWALL - VPN Policy Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: VPN Policy Name and Address

You must enter a name and the IPSec gateway name or address for this Policy.

Enter the name of this Policy and the peer IPSec gateway name or IP address and click Next to continue. The peer IPSec gateway name/address might be empty if it is a dynamic IP address, or can be given as a name that is resolvable via DNS.

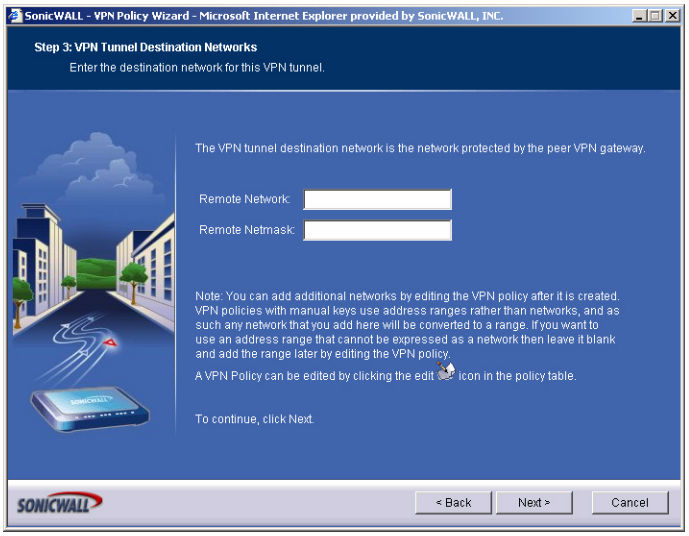
Policy Name:

IPSec Gateway Name or Address:

To continue, click Next.

3 Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully

Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.



SonicWALL - VPN Policy Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Step 3: VPN Tunnel Destination Networks
Enter the destination network for this VPN tunnel.
Remote Network:
Remote Netmask:
< Back
Next >
Cancel
SONICWALL

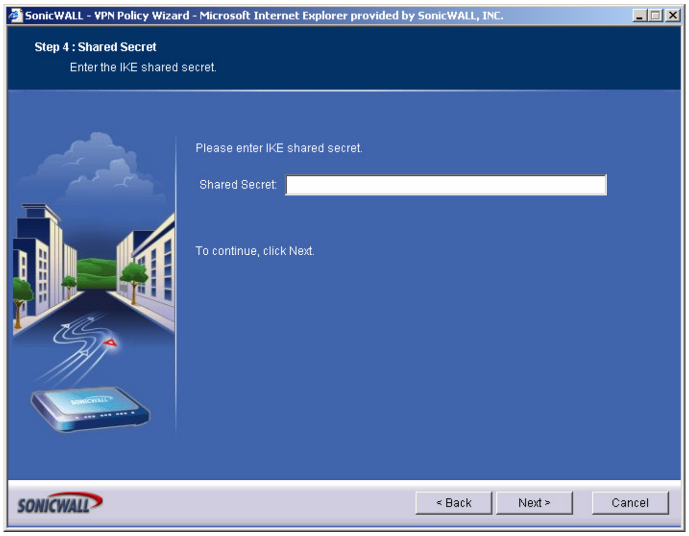
The VPN tunnel destination network is the network protected by the peer VPN gateway.

Note: You can add additional networks by editing the VPN policy after it is created. VPN policies with manual keys use address ranges rather than networks, and as such any network that you add here will be converted to a range. If you want to use an address range that cannot be expressed as a network then leave it blank and add the range later by editing the VPN policy.

A VPN Policy can be edited by clicking the edit icon in the policy table.

To continue, click Next.

4 Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.



SonicWALL - VPN Policy Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Step 4 : Shared Secret
Enter the IKE shared secret.
Shared Secret:
< Back
Next >
Cancel
SONICWALL

Please enter IKE shared secret.

To continue, click Next.

5 Enter a shared secret in the **Shared Secret** field. Use a combination of letters and numbers to create a unique secret. Click **Next**.

6 To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

Creating a Custom VPN Policy IKE with Preshared Secret

To create a custom VPN policy using IKE and a Preshared Secret, follow these steps:

1 Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.

2 Select **Custom**, and click **Next**.

3 Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully

Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.

4 Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.

Note: *You can add additional networks by editing the VPN policy after it is created in the VPN Policy Wizard.*

5 Select **IKE using Preshared Secret** as the IPSec Keying Mode. Click **Next**.

6 Enter a shared secret in the **Shared Secret** field. Use a combination of letters and numbers to create a unique secret. Click **Next**.

7 Select from the **DH Group** menu. Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process to establish pre-shared keys. To compromise between network speed and network security, select **Group 2**.

Select an encryption method from the **Encryption** list for the VPN tunnel. If network speed is preferred, then select **DES**. If network security is preferred, select **3DES**. To compromise between network speed and network security, select **DES**.

Select an authentication method from the **Authentication** list. SHA1 is preferred for network security.

Keep the default value of 28800 (8 hours) as the **Life Time (seconds)** for the VPN Policy. Click **Next**.

8 Select **ESP** from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

Select **3DES** from the **Encryption** menu. **3DES** is extremely secure and recommended for use.

Select **SHA1** from the **Authentication** menu.

Select **Enable Perfect Forward Secrecy**. The **Enable Perfect Forward Secrecy** check box increases the renegotiation time of the VPN tunnel. By enabling **Perfect Forward Secrecy**, a hacker using brute force to break encryption keys is not able to obtain other or future IPSec keys. During the phase 2 renegotiation between two SonicWALL appliances or a Group VPN SA, an additional Diffie-Hellman key exchange is performed. **Enable Perfect Forward Secrecy** adds incremental security between gateways.

If **Enable Perfect Forward Secrecy** is enabled, select the type of Diffie-Hellman (DH) Key Exchange (a key agreement protocol) to be used during phase 2 of the authentication process to establish pre-shared keys.

Leave the default value, 28800, in the **Life Time (seconds)** field. The keys renegotiate every 8 hours.

Click **Next**.

9 To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

Creating a Manual Key VPN Policy with the VPN Policy Wizard

You can create a custom VPN Policy using the VPN Wizard to configure a different IPSec method or configure more advanced features for the VPN Policy.

1 Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.

2 Select **Custom**, and click **Next**.

3 Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully

Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.

4 Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.

Note: *You can add additional networks by editing the VPN policy after it is created in the VPN Policy Wizard.*

5 Select **Manual Key** from the **IPSec Keying Modes** list. Click **Next**.

6 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length. Or use the default values.

Alert: *Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.*

ESP is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

3DES is selected by default from the **Encryption Method** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

The default 48-character key is a unique key generated every time a VPN Policy is created.

AH is selected by default from the **Authentication Key** field. When a new SA is created, a 32-character key is automatically generated in the **Authentication Key** field. This key can be used as a valid key. If this key is used, it must also be entered in the **Authentication Key** field in the remote SonicWALL. If authentication is not used, this field is ignored.

Click **Next**.

7 To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

Configuring IKE 3rd Party Certificates with the VPN Policy Wizard

Alert: *You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate. See* ***Chapter 40, Managing Certificates*** *for more information.*

1 Click **VPN Policy Wizard** to launch the wizard. Click **Next** to continue.

2 Select **Custom**, and click **Next**.

3 Enter a name for the policy in the **Policy Name** field. You may want to use the name of a remote office or other identifying feature so that it is easily identified. Enter the IP address or Fully Qualified Domain Name of the remote destination in the **IPSec Gateway Name or Address** field. Click **Next**.

4 Enter the IP address of the network protected by the remote SonicWALL in the **Remote Network** field. This is a private IP address on the remote network. Enter the subnet mask in the **Remote Netmask** field. Click **Next**.

5 Select **IKE using 3rd Party Certificates** from the **IPSec Keying Modes** list. Click **Next**.

6 Select your third party certificate from the **Third Party Certificate** menu. Select the ID type from the **Peer Certificate's ID Type**, and enter the ID string in the **ID string to match** field. Click **Next**.

7 Select from the **DH Group** menu. Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process to establish pre-shared keys. To compromise between network speed and network security, select **Group 2**.

Select an encryption method from the **Encryption** list for the VPN tunnel. If network speed is preferred, then select **DES**. If network security is preferred, select **3DES**. To compromise between network speed and network security, select **DES**.

Select an authentication method from the **Authentication** list. SHA1 is preferred for network security.

Leave the default value of 28800 (8 hours) as the **Life Time (seconds)** for the VPN Policy.

Click **Next**.

8. **ESP** is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.

   3DES is selected by default from the **Encryption** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

   The default 48-character key is a unique key generated every time a VPN Policy is created.

   AH is selected by default from the **Authentication Key** field. When a new SA is created, a 32-character key is automatically generated in the **Authentication Key** field. This key can be used as a valid key. If this key is used, it must also be entered in the **Authentication Key** field in the remote SonicWALL. If authentication is not used, this field is ignored.

   Click **Next**.

9. To enable the VPN policy immediately, click **Apply**. If you prefer to disable the policy initially, select **Create this Policy Disabled**, and then click **Apply**.

Creating Site-to-Site VPN Policies Using the VPN Policy Window

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPSec Keying mode VPN policies:

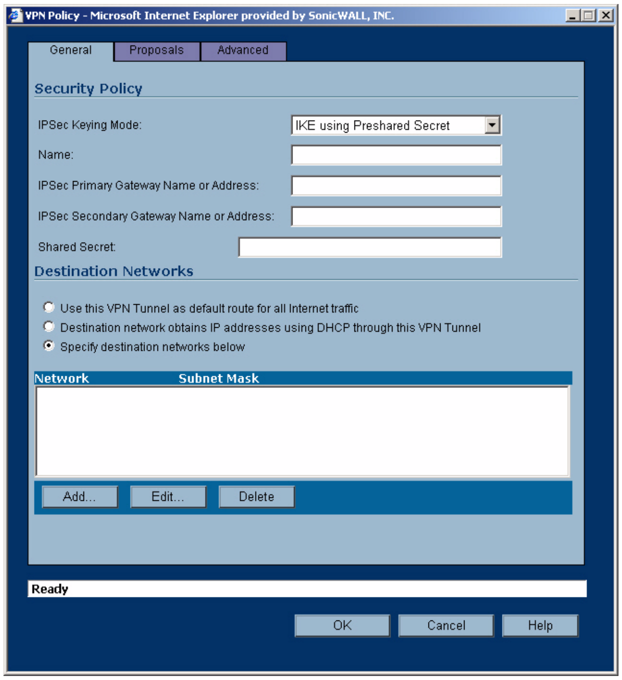
- IKE using Preshared Key
- Manual Key
- IKE using 3rd Party Certificates

✓ **Tip:** *You can create these policies using the VPN Policy Wizard.*

Configuring a VPN Policy IKE with Preshared Secret

To manually configure a VPN Policy using IKE with Preshared Secret, follow the steps below:

1 In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Security Policy
Name:
IPSec Primary Gateway Name or Address:
IPSec Secondary Gateway Name or Address:
Shared Secret:
Destination Networks
Network
Subnet Mask
Add...
Edit...
Delete
Ready
OK
Cancel
Help

IPSec Keying Mode: IKE using Preshared Secret

○ Use this VPN Tunnel as default route for all Internet traffic
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel
● Specify destination networks below

2 In the **General** tab**, IKE using Preshared Secret** is selected by default from the **IPSec Keying Mode** menu.

✓ **Tip:** *Use the VPN worksheet in this chapter to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.*

3 Enter a name for the VPN Policy in the **Name** field.

4 Enter the IP address or gateway name of the REMOTE SonicWALL in the **IPSec Primary Gateway Name or Address** field.

5 If you have a second IP address or gateway name, enter it in the **IPSec Secondary Gateway Name or Address** field. If the primary gateway is unavailable, the SonicWALL uses the second gateway to create the VPN tunnel.

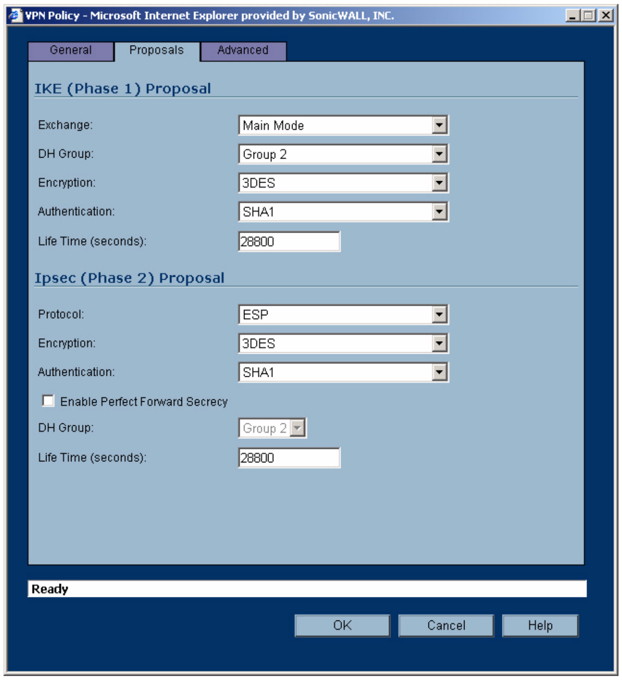
6 Enter a combination of letters, symbols, and numbers as the Shared Secret in the **Shared Secret** field.

✓ **Tip:** *The Shared Secret must be a minimum of four characters.*

7 Choose from the following options in the **Destination Networks** section:

- **Use this VPN Tunnel as the default route for all Internet traffic** - select this option if all local users access the Internet through this tunnel. You can only configure one tunnel to use this option.
- **Destination network obtains IP addresses using DCHP through this VPN Tunnel** - select this option if you are managing your network IP address allocation from a central location.
- **Specify destination networks below** - configure the remote destination network for your SA. Click **Add** to add the IP address and subnet mask. You can modify existing destination networks by click **Edit**, and delete networks by selecting the network and clicking **Delete**.

8 Click the **Proposals** tab.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

DH Group: Group 2

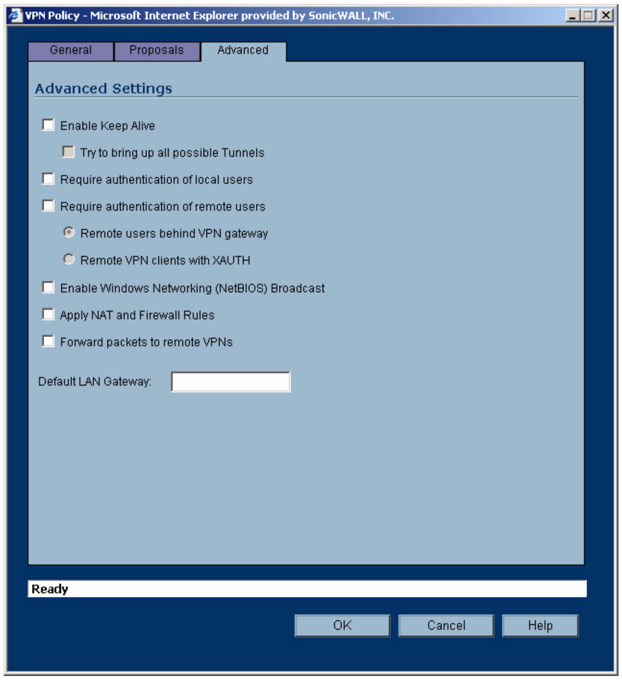
Life Time (seconds): 28800

Ready

9 In the **IKE (Phase 1) Proposal** section, the default settings offer a secure connection configuration, however, the settings can be modified to reflect your preferences. In addition to 3DES, AES-128, AES-192, and AES-256 can be selected for encryption methods.

10 In the **Ipsec (Phase 2) Proposal** section, the default settings offer a secure connection configuration, however, the settings can be modified to reflect your preferences. In addition to 3DES, AES-128, AES-192, and AES-256 can be selected for encryption methods. Selecting **Enable Perfect Forward Secrecy** prevents a hacker using brute force to break encryption keys from obtaining the current and future IPSec keys. During Phase 2 negotiation, an additional Diffie-Hellman key exchange is performed. This option adds an additional layer of security to the VPN tunnel.

11 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy in the **Advanced Settings** section.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Ready
OK
Cancel
Help

Advanced Settings

☐ Enable Keep Alive
  ☐ Try to bring up all possible Tunnels
☐ Require authentication of local users
☐ Require authentication of remote users
  ● Remote users behind VPN gateway
  ○ Remote VPN clients with XAUTH
☐ Enable Windows Networking (NetBIOS) Broadcast
☐ Apply NAT and Firewall Rules
☐ Forward packets to remote VPNs

Default LAN Gateway:

- **Enable Keep Alive** - Select this setting if you want to maintain the current connection by listening for traffic on the network segment between the two connections. If multiple VPN tunnels are configured on the SonicWALL, select Try to bring up all possible tunnels to have the SonicWALL renegotiate the tunnels if they lose communication with the SonicWALL.
- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users** - requires all inbound VPN traffic for this SA is from an authenticated user. Select **Remote users behind VPN gateway** if remote users have a VPN tunnel that terminates on the VPN gateway. Select **Remote VPN clients with XAUTH** if remote users require authentication using XAUTH and are access the SonicWALL via a VPN clients.
- **Enable Secure Wireless Bridging** - enables a WiFiSec VPN policy between SonicWALL wireless gateways.
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site’s LAN subnet to be hidden from the corporate site, and is most useful when a remote office’s network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the **Routing** page located in the **Network** section. Enabling this feature allows a network administrator to create a “hub and spoke” network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a “hub and spoke” network, select the **Forward Packets to Remote**

VPNs check box.Traffic can travel from a branch office to a branch office via the corporate office.

- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all internet traffic through this SA check box. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ/WLAN, or LAN/OPT/DMZ/WLAN** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ/WLAN network.

12. Click **OK**. Your new VPN policy is displayed in the **VPN Policies** table.

Configuring a VPN Policy using Manual Key

To manually configure a VPN Policy in the **VPN Policy** window using Manual Key, follow the steps below:

1. In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.
2. Select **Manual Key** from the **IPSec Keying Mode** menu.

Tip: *Use the VPN worksheet at the beginning of this chapter to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.*

3. In the **Security Policy** section, enter a name for the VPN Policy in the **Name** field.
4. Enter the IP address or gateway name of the REMOTE SonicWALL in the **IPSec Gateway Name or Address** field.
5. In the **Destination Networks** section, one of the following options:
    - **Use this VPN Tunnel as the default route for all Internet traffic** - select this option if all local users access the Internet through this tunnel. You can only configure one SA to use this option.
    - **Specify destination networks below** - configure the remote destination network for your SA. Click **Add** to add the IP address and subnet mask. You can modify existing destination networks by click **Edit**, and delete networks by selecting the network and clicking **Delete**.
6. Click on the **Proposals** tab.
7. In the **Ipsec SA** section, define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length. Or use the default values.

Alert: *Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.*

8. **ESP** is selected by default from the **Protocol** menu. ESP is more secure than AH, but AH requires less processing overhead.
9. **3DES** is selected by default from the **Phase 2 Encryption** menu. Enter a 48-character hexadecimal key if you are using 3DES encryption.Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. This encryption key must match the remote SonicWALL's encryption key.

    The default 48-character key is a unique key generated every time a VPN Policy is created.
10. **SHA1** is selected by default from the **Phase 2 Authentication** menu. When a new Policy is created, a 32-character key is automatically generated in the **Authentication Key** field. This key

can be used as a valid key. If this key is used, it must also be entered in the **Authentication Key** field in the remote SonicWALL. If authentication is not used, this field is ignored.

11 Click on the **Advanced** tab. Select the optional configuration settings you want to apply to your VPN policy from the **Advanced Settings** section.

- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users -** requires all inbound VPN traffic for this SA is from an authenticated user.
- **Enable Secure Wireless Bridging** -
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.
- **Forward Packets to Remote VPNs -** allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the **Routing** page located in the **Network** section. Enabling this feature allows a network administrator to create a "hub and spoke" network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a "hub and spoke" network, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the **Use this VPN Tunnel as the default route for all internet traffic**. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this VPN Policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ/WLAN, or LAN/OPT/DMZ/WLAN -** Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ/WLAN network.

12 Click **OK** to add the Manual Key VPN Policy to the SonicWALL.

Configuring a VPN Policy with IKE 3rd Party Certificate

▲ **Alert:** *You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate. See* ***Chapter 40, Managing Certificates*** *for more information.*

To create a VPN SA using IKE and third party certificates, follow these steps:

1 In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.

2 In **General** tab, select **IKE using 3rd Party Certificates**.

3 Type a Name for the Security Association in the **Name** field.

4 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPSec Primary Gateway Name or Address** field. If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPSec Secondary Gateway Name or Address** field.

5 Select a certificate from the **Third Party Certificate** menu.

6 Select one of the following Peer ID types from the **Peer ID Type** menu and enter an ID string in the **ID string to match** field.

E-Mail ID and Domain Name - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The certificate verification process did not actually verify my email address or domain name, just that the certificate I selected to use, had this matching entry contained in the Alternative Subject Name field. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

Distinguished Name **-** based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). Up to three organizational units can be specified. The usage is c=*;o=*;ou=*;ou=*;ou=*;cn=*. The final entry does not need to contain a
semi-colon. You must enter at least one entry, i.e. c=us.

7 In the **Destination Network** section, select one of the following options:

Use this VPN Tunnel as default route for all Internet traffic - select this option if you don’t want any local user to leave the SonicWALL security appliance unless the traffic goes through a VPN tunnel.

Destination network obtains IP addresses using DHCP through this VPN Tunnel - Select this setting if you want the remote network to obtain IP addresses from your DHCP server.

Specify destination networks below - allows you to add the destination network or networks. To add a destination network, click **Add**. The **Edit VPN Destination Network** window is displayed. Enter the IP address in the **Network** field and the subnet in the **Subnet Mask** field, then click **OK**.

8 Click the **Proposals** tab.

9 In the **IKE (Phase 1) Proposal** section, select the following settings:

Select **Aggressive Mode** from the **Exchange** menu.

Select **Group 2** from the **DH Group** menu.

Select **3DES** from the **Encryption** menu.

Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

10 In the Ipsec (Phase 2) Proposal section, select the following settings:

Select **ESP** from the **Protocol** menu.

Select **3DES** from the **Encryption** menu.

Select **SHA1** from the **Authentication** menu.

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security, then select **Group 2** from the **DH Group** menu.

Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

11 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy in the **Advanced Settings** section.

- Enable Keep Alive - Select this setting if you want to maintain the current connection by listening for traffic on the network segment between the two connections. If multiple VPN tunnels are configured on the SonicWALL, select Try to bring up all possible tunnels to have the SonicWALL renegotiate the tunnels if they lose communication with the SonicWALL.
- **Require authentication of local users** - requires all outbound VPN traffic from this SA is from an authenticated source.
- **Require authentication of remote users** - requires all inbound VPN traffic for this SA is from an authenticated user. Select **Remote users behind VPN gateway** if remote users have a VPN tunnel that terminates on the VPN gateway. Select **Remote VPN clients with XAUTH** if remote users require authentication using XAUTH and are access the SonicWALL via a VPN clients.
- **Enable Secure wireless Bridging Mode** -
- **Enable Windows Networking (NetBIOS) broadcast** - to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- **Apply NAT and Firewall Rules** - This feature allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.
- **Forward Packets to Remote VPNs** - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the **Routing** page located in the **Network** section. Enabling this feature allows a network administrator to create a "hub and spoke" network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a "hub and spoke" network, select the **Forward Packets to Remote VPNs** check box.Traffic can travel from a branch office to a branch office via the corporate office.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the Route all internet traffic through this SA check box. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **VPN Terminated at the LAN, OPT/DMZ/WLAN, or LAN/OPT/DMZ/WLAN** - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific destination, the VPN tunnel has access to a specific portion of the destination LAN or OPT/DMZ/WLAN network.

12 Click **OK**. Your new VPN policy is displayed in the **VPN Policies** table.

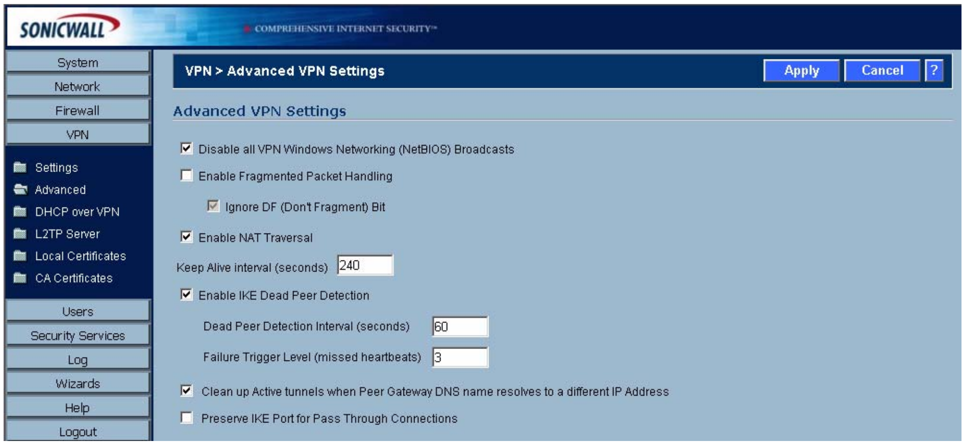
CHAPTER

37

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
VPN > Advanced VPN Settings
Apply
Cancel
?

Advanced VPN Settings

☑ Disable all VPN Windows Networking (NetBIOS) Broadcasts

☐ Enable Fragmented Packet Handling

☑ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

Keep Alive interval (seconds) 240

☑ Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds) 60

Failure Trigger Level (missed heartbeats) 3

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

☐ Preserve IKE Port for Pass Through Connections

Advanced VPN Settings

- **Disable all VPN Windows Networking (NetBIOS) Broadcasts** - Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. Disable this setting access remote network resources by browsing the Windows®
Network Neighborhood.
- **Enable Fragmented Packet Handling** - if the VPN log report shows the log message "Fragmented IPSec packet dropped", select this feature. Do not select it until the VPN tunnel is established and in operation. When you select this setting, the **Ignore DF (Don't Fragment) Bit** setting becomes active.
- **Enable NAT Traversal** - Select this setting is a NAT device is located between your VPN endpoints. IPSec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPSec session, a 1-byte UDP is designated as a

keep alive that acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPSec peer.

Selecting **Enable NAT Traversal** allows VPN tunnels to support this protocol, and log messages are generated by the SonicWALL when a IPSec Security Gateway is detected behind a NAT/ NAPT device. The following log messages are found on the **View > Log** page:

Peer IPSec Gateway behind a NAT/NAPT device

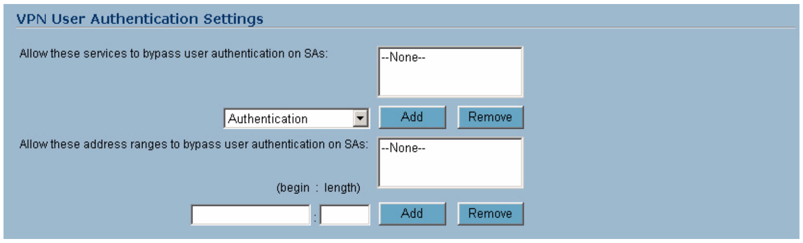
Local IPSec Security Gateway behind a NAT/NAPT device

No NAT/NAPT device detected between IPSec Security

Peer IPSec Security Gateway doesn’t support VPN NAT Traversal

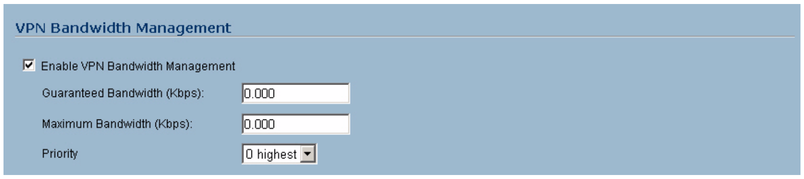
- **Keep Alive interval (seconds)** - the default value is 240 seconds (4 minutes). If **Enable Keep Alive** is selected on the **Advanced VPN Settings** page, a new negotiation begins if the previous VPN Policy was deleted by Dead Peer Detection (DPD).
- **Enable IKE Dead Peer Detection** - select if you want inactive VPN tunnels to be dropped by the SonicWALL. Enter the number of seconds between “heartbeats” in the **Dead Peer Detection Interval (seconds)** field. The default value is 60 seconds. Enter the number of missed heartbeats in the **Failure Trigger Level (missed heartbeats)** field. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
- **VPN Single Armed mode (stand-alone VPN gateway)** -
- **Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass Through Connections** - Preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.

VPN User Authentication Settings


VPN User Authentication Settings
Allow these services to bypass user authentication on SAs:
--None--
Authentication
Add
Remove
Allow these address ranges to bypass user authentication on SAs:
--None--
(begin : length)
Add
Remove

- **Allow these services to bypass user authentication on SAs** - this feature allows VPN users without authentication to access the specified services. To add a service, select the service from the menu and click **Add**. The service is added to the **Allow these services to bypass user authentication on SAs** list. To remove a service, select the service in the **Allow these services to bypass user authentication on VPN SAs** list and click **Remove**.
- **Allow these address ranges to bypass user authentication on SAs** - this feature allows the specified IP address or IP address range to bypass user authentication on VPN connections. To add an IP address, enter the single IP address in the text box, then click **Add**. To add an IP address range, enter the range starting IP address in the first field and the length in the text field (up to the last three numbers of the IP address).

VPN Bandwidth Management



VPN Bandwidth Management

☑ Enable VPN Bandwidth Management

Guaranteed Bandwidth (Kbps): 0.000

Maximum Bandwidth (Kbps): 0.000

Priority: 0 highest

Bandwidth management is a means of allocating bandwidth resources to critical applications on a network. The **VPN Bandwidth Management** section allows you to define the amount of outbound VPN traffic allowed from the SonicWALL. Traffic is then scheduled in Kbps according to **Guaranteed Bandwidth** (minimum) and **Maximum Bandwidth** settings.

To enable VPN Bandwidth Management, follow these steps:

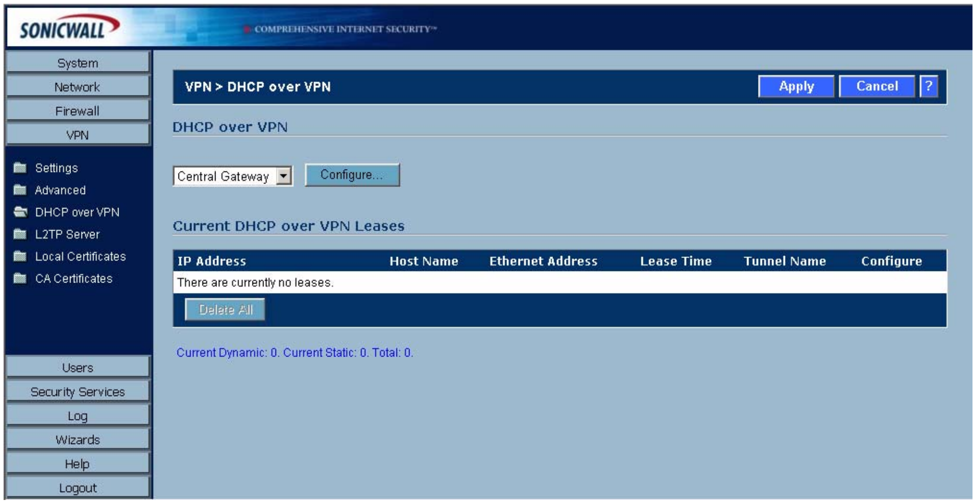
1. Select **Enable VPN Bandwidth Management**.
2. Enter the minimum amount of bandwidth allowed in the **Guaranteed Bandwidth (Kbps)** field.
3. Enter the maximum amount of bandwidth allowed in **Maximum Bandwidth** (Kbps) field.
4. Select VPN bandwidth priority from the **Priority** menu, **0 (highest)** to **7 (lowest)**.
5. Click Apply.

Tip: *Bandwidth management is available only on outbound VPN traffic. You cannot configure individual Security Associations to use bandwidth management.*

CHAPTER 38

Configuring DHCP Over VPN

VPN > DHCP over VPN


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
VPN > DHCP over VPN
Apply
Cancel
?
DHCP over VPN
Configure...
Current DHCP over VPN Leases
Delete All

Central Gateway

IP Address	Host Name	Ethernet Address	Lease Time	Tunnel Name	Configure
There are currently no leases.					

Current Dynamic: 0. Current Static: 0. Total: 0.

The **VPN > DHCP over VPN** page allows a Host (DHCP Client) behind a SonicWALL obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

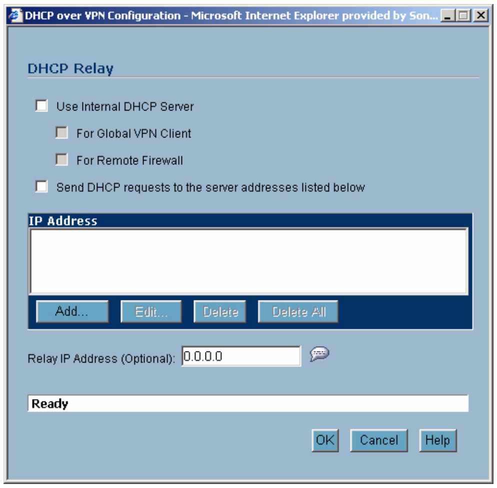
DHCP Relay Mode

The SonicWALL appliance at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The SonicWALL at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The SonicWALL at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Configuring the Central Gateway for DHCP Over VPN

To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

1. On the **DHCP over VPN** page, select **Central Gateway** from the **DHCP Relay Mode** menu.
2. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.


DHCP over VPN Configuration - Microsoft Internet Explorer provided by Son...
DHCP Relay
IP Address
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

☐ Use Internal DHCP Server
  ☐ For Global VPN Client
  ☐ For Remote Firewall
☐ Send DHCP requests to the server addresses listed below

Relay IP Address (Optional): 0.0.0.0

Ready

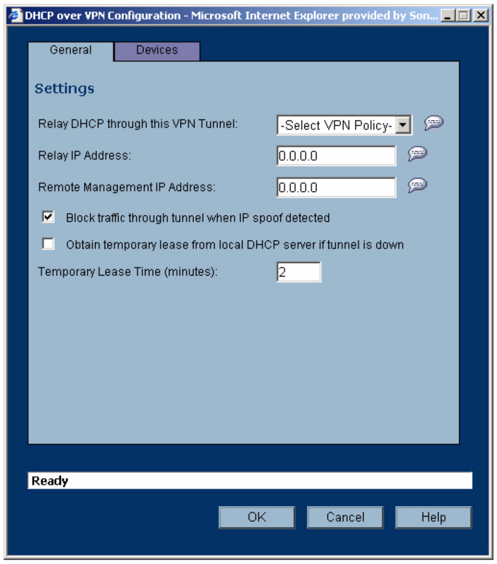
3. Select **Use Internal DHCP Server** to enable the Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information.
4. If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
5. Click **Add**. The IP Address window is displayed.
6. Enter the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL now directs DHCP requests to the specified servers.
7. Enter the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

Configuring DHCP over VPN Remote Gateway

1 Select **Remote Gateway** from the **DHCP Relay Mode** menu.

2 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



DHCP over VPN Configuration - Microsoft Internet Explorer provided by Son...
General
Devices
OK
Cancel
Help

Settings

Relay DHCP through this VPN Tunnel: -Select VPN Policy-

Relay IP Address: 0.0.0.0

Remote Management IP Address: 0.0.0.0

☑ Block traffic through tunnel when IP spoof detected

☐ Obtain temporary lease from local DHCP server if tunnel is down

Temporary Lease Time (minutes): 2

Ready

3 Select the VPN Security Association to be used for the VPN tunnel from the **Relay DHCP through this VPN Tunnel** menu.

Alert: *Only VPN Security Associations using IKE and terminate on the LAN appear in the Obtain using DHCP through this VPN Tunnel.*

4 The **Relay IP address** is used in place of the Central Gateway address, and must be reserved in the DHCP scope on the DHCP server. The Relay IP address can also be used to manage the SonicWALL remotely through the VPN tunnel behind the Central Gateway.

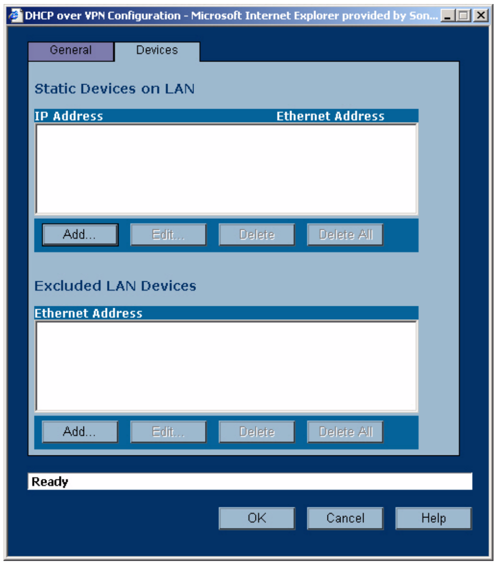
5 The **Remote Management IP Address,** if entered, can be used to manage the SonicWALL remotely through the VPN tunnel behind the Central Gateway.

6 If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is entered for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL to respond to IP spoofs.

7 If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, enter the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is two (2) minutes.

Device Configuration

1 To configure devices on your LAN, click the **Devices** tab.


DHCP over VPN Configuration - Microsoft Internet Explorer provided by Son...
General
Devices
Static Devices on LAN
IP Address
Ethernet Address
Add...
Edit...
Delete
Delete All
Excluded LAN Devices
Ethernet Address
Add...
Edit...
Delete
Delete All
Ready
OK
Cancel
Help

2 To configure **Static Devices on LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field. An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click **OK**.

3 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window. Enter the MAC address of the device in the **Ethernet Address** field. Click **OK**.

4 Click **OK** to exit the **DHCP over VPN Configuration** window.

▲ **Alert:** *You must configure the local DHCP server on the remote SonicWALL to assign IP leases to these computers.*

▲ **Alert:** *If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.*

✓ **Tip:** *If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.*

Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name. To edit an entry, click the edit icon under **Configure** for that entry.

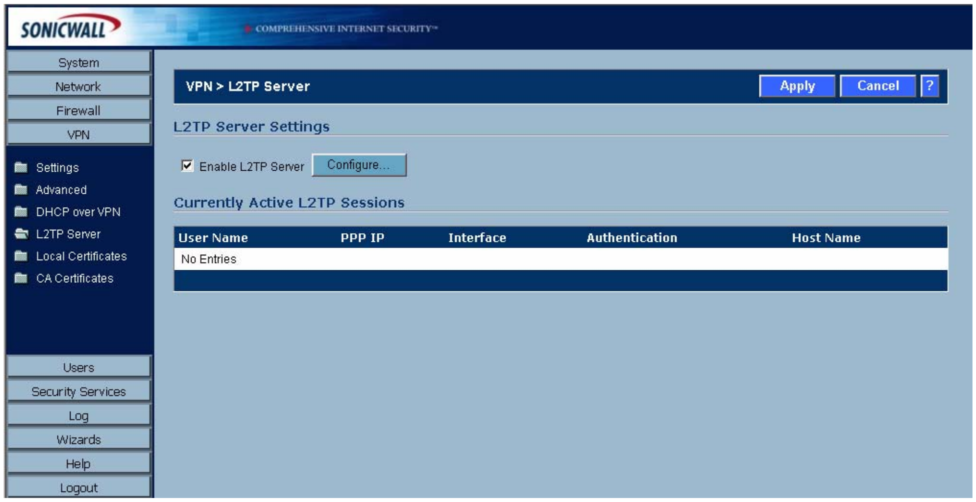
To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the Trashcon icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.

CHAPTER 39

Configuring L2TP Server Settings

VPN > L2TP Server


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Configure...

VPN > L2TP Server

L2TP Server Settings

☑ Enable L2TP Server

Currently Active L2TP Sessions

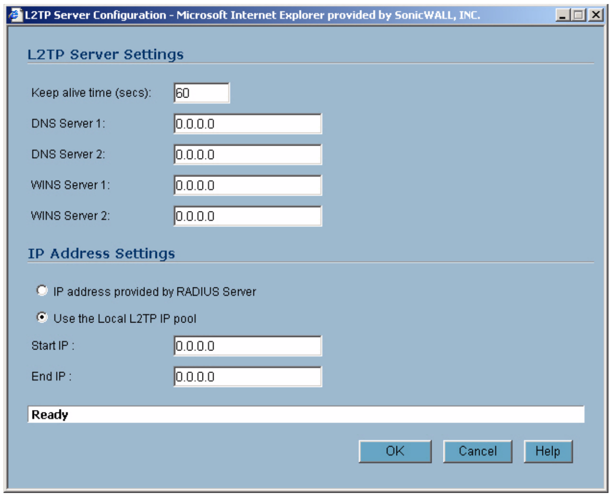
User Name	PPP IP	Interface	Authentication	Host Name
No Entries				

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPSec to provide a secure, encrypted VPN solution.

Note: *You must enable Group VPN before configuring the SonicWALL L2TP feature. Also, the encryption method and shared secret must match the L2TP client settings.*

To enable L2TP Server functionality on the SonicWALL, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.


L2TP Server Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.

L2TP Server Settings

Keep alive time (secs): 60
DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
WINS Server 1: 0.0.0.0
WINS Server 2: 0.0.0.0

IP Address Settings

○ IP address provided by RADIUS Server
● Use the Local L2TP IP pool
Start IP : 0.0.0.0
End IP : 0.0.0.0

Ready

L2TP Server Settings

Configure the following settings:

1 Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open.

2 Enter the IP address of your first DNS server in the **DNS Server 1** field.

3 If you have a second DNS server, enter the IP address in the **DNS Server 2** field.

4 Enter the IP address of your first WINS server in the **WINS Server 1** field.

5 If you have a second WINS server, enter the IP address in the **WINS Server 2** field.

IP Address Settings

6 Select **IP address provided by RADIUS Server** if a RADIUS Server provides IP addressing information to the L2TP clients.

7 If the L2TP Server provides IP addresses, select **Use the Local L2TP IP** pool. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.

8 Click **OK**.

Adding L2TP Clients to the SonicWALL

To add L2TP clients to the local user database or a RADIUS database, click **Users,** then **Add**. When adding privileges for a user, select **L2TP Client** as one of the privileges. Then the user can access the SonicWALL as a L2TP client.

Currently Active L2TP Sessions

- **User Name** - the user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - the source IP address of the connection.
- **Interface** - the enter of interface used to access the L2TP Server, whether it’s a VPN client or another SonicWALL appliance.
- **Authentication** - enter of authentication used by the L2TP client.
- **Host Name** - the name of the network connecting to the L2TP Server.

CHAPTER 40

Managing Certificates

Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange VPN policy. IKE is an important part of IPSec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

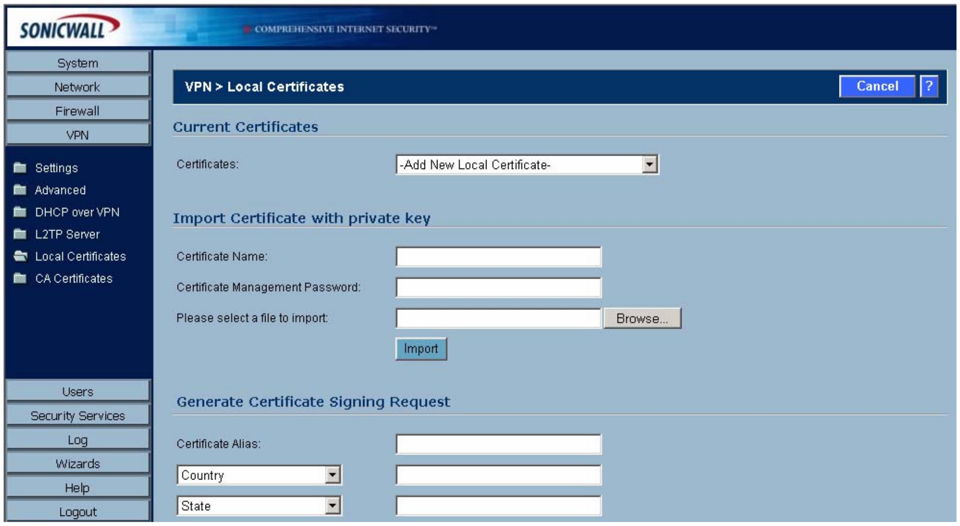
SonicWALL Third-Party Digital Certificate Support

SonicWALL supports third party certificates from the following two vendors of Certificate Authority Certificates:

- VeriSign
- Entrust

To implement the use of certificates for VPN SAs, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL to validate your Local Certificates. You import the valid CA certificate into the SonicWALL using the **VPN > CA Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates you add in the **VPN > Local Certificates** page.

VPN > Local Certificates


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
VPN > Local Certificates
Cancel
?
Current Certificates
Import Certificate with private key
Certificate Name:
Certificate Management Password:
Please select a file to import:
Browse...
Import
Generate Certificate Signing Request
Certificate Alias:

Certificates: -Add New Local Certificate-

Country

State

After a certificate is signed by the CA and returned to you, you can import the certificate into the SonicWALL to be used as a **Local Certificate** for a VPN Security Association.

✓ **Tip:** *After you import a local certificate on the SonicWALL, it is recommended you export the certificate to the local disk as a backup. When exporting a local certificate, a password is required.*

Importing Certificate with Private Key

Use the following steps to import the certificate into the SonicWALL:

1. In the **Import Certificate with private key** section of **Local Certificates**, type the **Certificate Name**.
2. Type the **Certificate Management Password**. This password was created when you exported your signed certificate.
3. Use **Browse** to locate the certificate file.
4. Click **Import**, and the certificate appears in the list of **Current Certificates**.
5. To view details about the certificate, select it from the list of **Current Certificates**.

Certificate Details

To view details about the certificate, select the certificate from the **Certificates** menu in the **Current Certificates** section. The Certificate Details section lists the following information about the certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Expiration On
- Alternate Subject Name
- Alternate Subject Name Type
- Status

Delete This Certificate

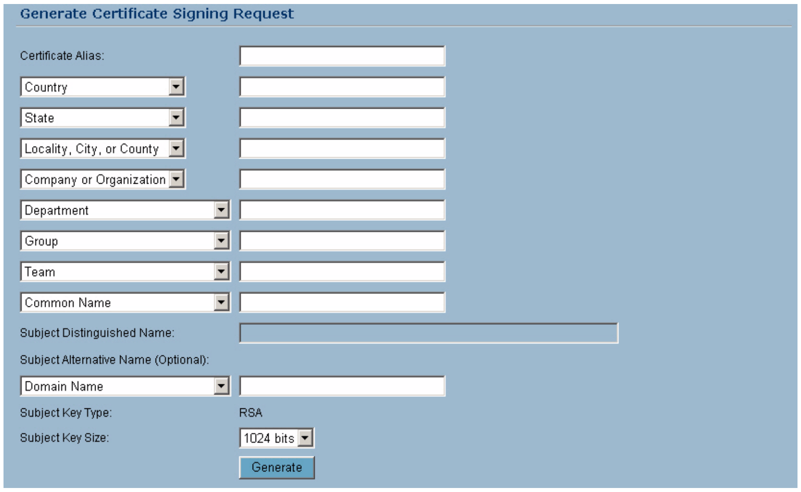
To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Generating a Certificate Signing Request

To generate a local certificate for use with a VPN policy, follow these steps:

✓ **Tip:** *You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.*

1 Select **Add New Local Certificate** from the **Certificates** menu.


Generate Certificate Signing Request
Certificate Alias:
Country
State
Locality, City, or County
Company or Organization
Department
Group
Team
Common Name
Subject Distinguished Name:
Subject Alternative Name (Optional):
Domain Name
Subject Key Type:
RSA
Subject Key Size:
1024 bits
Generate

2 In the **Generate Certificate Signing Request** section, enter a name for the certificate in the **Certificate Name** field.

3 Enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**. You need to provide the proper input for the **Domain Name** (yourcompanyname.com) or **E-mail Address** (abc@yourcompanyname.com) option in the corresponding field.

4 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

5 Select a Subject Key size from the **Subject Key Size** menu.

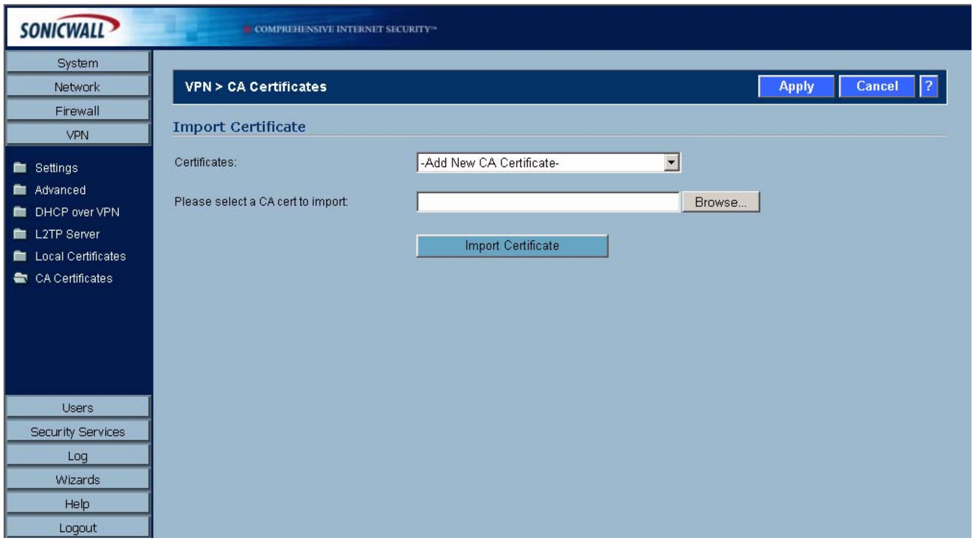
Note: *Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for support key sizes.*

6 Click **Generate** to create a certificate file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.

7 Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

VPN > CA Certificates


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Security Services
Log
Wizards
Help
Logout
VPN > CA Certificates
Apply
Cancel
?
Import Certificate
Certificates:
-Add New CA Certificate-
Please select a CA cert to import:
Browse...
Import Certificate

Importing CA Certificates into the SonicWALL

After your CA service has validated your **CA Certificate**, you can import it into the SonicWALL and use it to validate **Local Certificates** for VPN Security Associations.

To import your **CA Certificate** into the SonicWALL, follow these steps:

1. Select **Add New CA Certificate**.
2. Click **Browse**, and locate the PKCS#7 (*.p7b) or DER (*.der) or *.cer encoded file sent by the CA service.
3. Click **Open** to set the directory path to the certificate
4. Click **Import** to import the certificate into the SonicWALL. Once it is imported, you can view the **Certificate Details**.

Certificate Details

The **Certificate Details** section lists the following information:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Expires On
- CRL Status

The **Certificate Issuer**, **Certificate Serial Number**, and the **Expiration Date** are generated by the CA service. The information is used when a **Generate Certificate Signing Request** is created and sent to your CA service for validation.

Delete This Certificate

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Certificate Revocation List (CRL)

A **Certificate Revocation List (CRL)** is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- It is no longer needed.
- A certificate was stolen or compromised.
- A new certificate was issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a **Certificate Revocation List** at a given interval, or on an online server in a X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA provider for specific details on locating a CRL file or URL.

You can import the CRL by manually downloading the CRL and then importing it into the SonicWALL. You can also enter the URL location of the CRL by entering the address in the **Enter CRL's location (URL) for auto-import** field. The CRL is downloaded automatically at intervals determined by the CA service. Certificates are checked against the CRL by the SonicWALL for validity when they are used.

Importing a CRL List

To import a CRL list, follow these steps:

1. Click **Browse** for **Please select a file to import**.
2. Locate the PKCS#12 (*.p12) or Micorosft (*.pfx) encoded file.
3. Click **Open** to set the directory path to the certificate.
4. Click **Import** to import the certificate into the SonicWALL.

Automatic CRL Update

To enable automatic CRL updates to the SonicWALL, type the URL of the CRL server for your CA service in the **Enter CRL's location (URL) for auto-import**, then click Apply.

PART

9

Users

CHAPTER 41

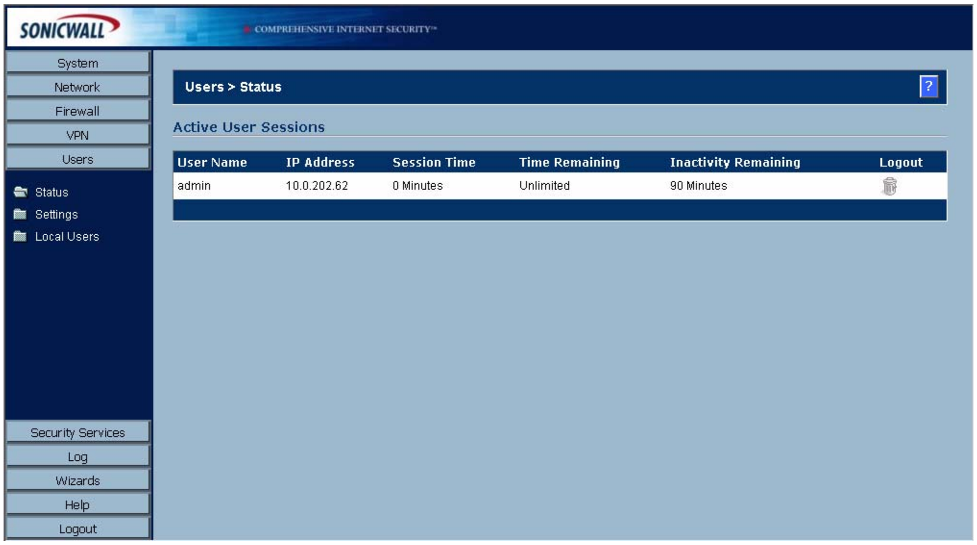
Viewing User Status and Configuring User Authentication

User Level Authentication Overview

The SonicWALL security appliance provides a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to bypass content filtering. Also, you can permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

User level authentication can performed using a local user database, RADIUS, or a combination of the two applications. The local database on the SonicWALL security appliance can support up to 1,000 users. If you have more than 1,000 users or want to add an extra layer of security for authenticating users to the SonicWALL security appliance, use RADIUS for authentication.

Users > Status


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Status
Settings
Local Users
Security Services
Log
Wizards
Help
Logout
Users > Status
?

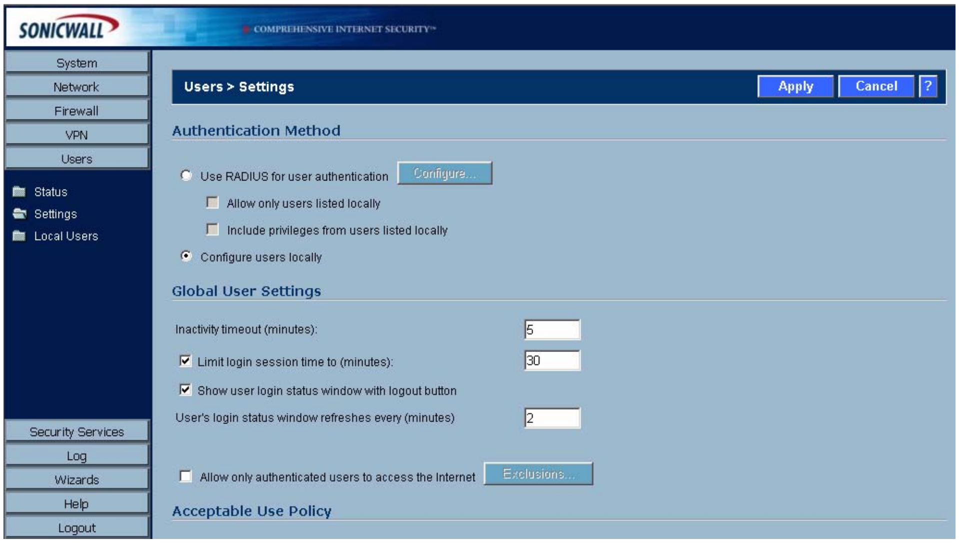
Active User Sessions

User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining	Logout
admin	10.0.202.62	0 Minutes	Unlimited	90 Minutes	🗑

Active User Sessions

The Active User Sessions table lists the **User Name**, the **IP Address** of the user, the **Session Time**, **Time Remaining** of the session, and the **Inactivity Remaining** time. You can also click the **Trashcan** icon in the **Logout** column to log a user out of the SonicWALL security appliance.

Users > Settings



Authentication Method

○ Use RADIUS for user authentication

☐ Allow only users listed locally

☐ Include privileges from users listed locally

● Configure users locally

Global User Settings

Inactivity timeout (minutes): 5

☑ Limit login session time to (minutes): 30

☑ Show user login status window with logout button

User's login status window refreshes every (minutes) 2

☐ Allow only authenticated users to access the Internet

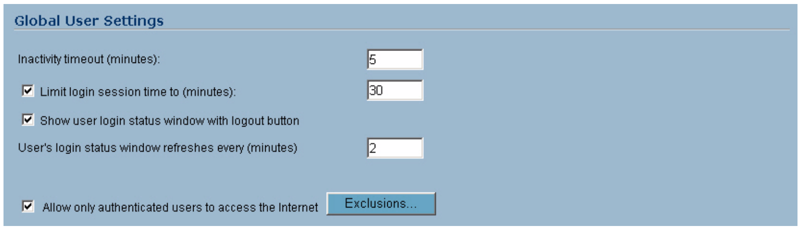
Acceptable Use Policy

On the Users > Settings page, you can configure the authentication method required, global user settings, and an acceptable use policy that is displayed to users when logging onto your network. The SonicWALL security appliance supports user level authentication using the local SonicWALL security appliance database, a RADIUS server, or a combination of the two authentication methods.

Authentication Method

- **Use RADIUS for user authentication** - if you have more than 100 users or want to add an extra layer of security for authenticating the user to the SonicWALL security appliance. If you select Use RADIUS for user authentication, users must log into the SonicWALL security appliance using HTTPS in order to encrypt the password sent to the SonicWALL security appliance. If a user attempts to log into the SonicWALL security appliance using HTTP, the browser is automatically redirected to HTTPS. If you select **Use RADIUS for user authentication**, the **Configure** button becomes available.
- **Allow only users listed locally** - enable this setting if you have a subset of RADIUS users accessing the SonicWALL security appliance. The user names must be added to the internal SonicWALL security appliance user database on the **Users > Local Users** page before they can be authenticated using RADIUS.
- **Include privileges from users listed locally** - includes the privileges assigned to users in the **Users > Local Users** page.
- **Configure users locally** - selecting this setting allows you to configure users in the local SonicWALL security appliance database using the **Users > Local Users** page.

Global User Settings



Global User Settings

Inactivity timeout (minutes): 5

☑ Limit login session time to (minutes): 30

☑ Show user login status window with logout button

User's login status window refreshes every (minutes) 2

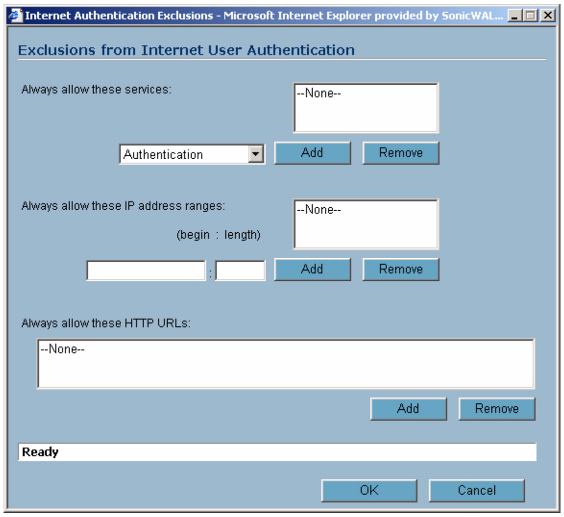
☑ Allow only authenticated users to access the Internet

The settings listed below apply to all users when authenticated through the SonicWALL security appliance.

- **Inactivity timeout (minutes)** - users can be logged out of the SonicWALL security appliance after a preconfigured inactivity time. Enter the number of minutes in this field.
- **Limit login session time to (minutes)** - you can limit the time a user is logged into the SonicWALL security appliance by selecting the check box and typing the amount of time, in minutes, in the **Limit login session time to (minutes)** field. The default value is **30** minutes.
- **Show user login status window with logout button** - displays a logout button in the user login status window.
- **User's login status window refreshes every (minutes)** - refreshes the user login status window based on the specified minutes.
- **Allow only authenticated users to access the Internet** - this feature allows Internet access to only users configured on the SonicWALL security appliance. When you check this setting, the **Exclusions** button becomes available. Clicking the Exclusions button displays the **Internet Authentication Exclusions** window.

Internet Authentication Exclusions

When you select **Allow only authenticated users to access the Internet**, and click the **Exclusions** button, the **Internet Authentication Exclusions** window is displayed for configuring exclusions from Internet User Authentication.



Internet Authentication Exclusions - Microsoft Internet Explorer provided by SonicWAL...

Exclusions from Internet User Authentication

Always allow these services: --None--

Authentication

Always allow these IP address ranges: --None--

(begin : length)

Always allow these HTTP URLs: --None--

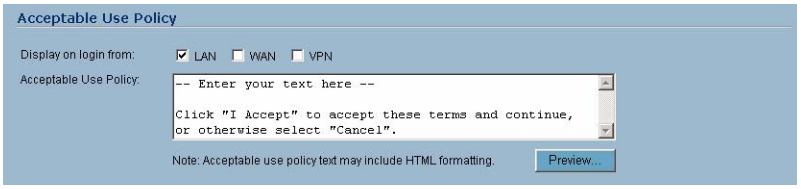
Ready

- **Always allow these services** - the default is **None**. You can add or remove services available to users. To add a service, select the service from the menu, and click **Add**. To remove a service, select the service in the in the services list, and click **Remove**.
- **Always allow these address ranges** - this feature allows the specified IP address or IP address range to bypass user authentication. To add an IP address, enter the single IP address in the first

field, then click **Add**. To add an IP address range, enter the range starting IP address in the first field and the length of the range in the next field (up to the last three numbers of the IP address.

- **Always allow these HTTP URLs** - this feature allows you to specify HTTP URLs to bypass user authentication. To add a URL, click the **Add** button. Enter the URL, then click **OK**. To remove a URL, select the URL entry, and click **Remove**.

Acceptable Use Policy



Acceptable Use Policy

Display on login from: ☑ LAN ☐ WAN ☐ VPN

Acceptable Use Policy:

```
-- Enter your text here --

Click "I Accept" to accept these terms and continue,
or otherwise select "Cancel".
```

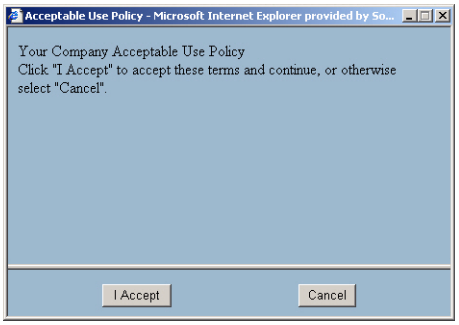
Note: Acceptable use policy text may include HTML formatting.

An acceptable use policy (AUP) is a policy users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL security appliance.

You can choose to display an acceptable use policy message when users log in by selecting the interface **LAN**, **WAN**, **DMZ**, **OPT**, **WLAN**, or **VPN** in the **Display on login** section. The **LAN** option is checked by default. If these settings are unchecked, no AUP is displayed.

In the **Acceptable Use Policy** field, enter the text of your policy where the placeholder text **-- Enter your text here --** is displayed. You can add HTML tags to format the page.

Click **Preview** to display the AUP window as it appears to users.



Acceptable Use Policy - Microsoft Internet Explorer provided by So...

Your Company Acceptable Use Policy
Click "I Accept" to accept these terms and continue, or otherwise select "Cancel".

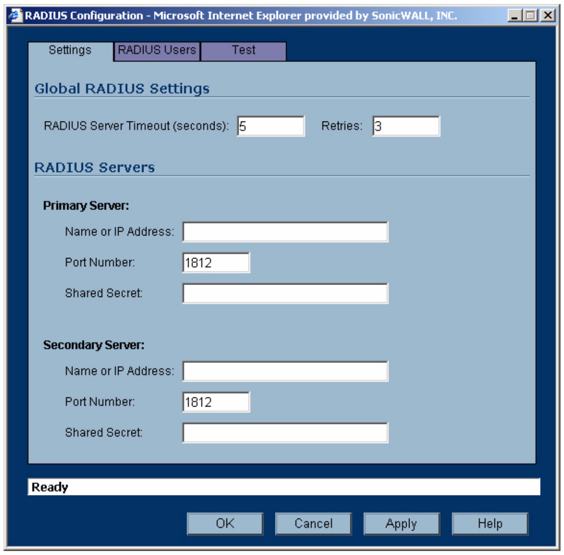
Click **Apply** to save your AUP message.

Tip: *Acceptable Use Policies can use HTML formatting in the body of the message.*

Configuring RADIUS Authentication

To enable the SonicWALL security appliance to use authentication from a RADIUS server, follow these steps:

1. Select **Use RADIUS for user authentication**.
2. Select **Allow only users listed locally** if only the users listed in the SonicWALL security appliance database are authenticated using RADIUS.
3. Click **Configure** to set up your RADIUS server settings on the SonicWALL security appliance. The **RADIUS Configuration** window is displayed.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
Ready
OK
Cancel
Apply
Help

Global RADIUS Settings

RADIUS Server Timeout (seconds): 5
Retries: 3

RADIUS Servers

Primary Server:

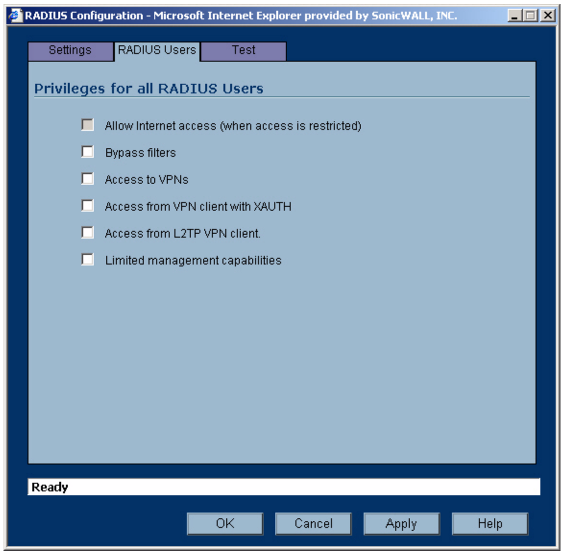
Name or IP Address:
Port Number: 1812
Shared Secret:

Secondary Server:

Name or IP Address:
Port Number: 1812
Shared Secret:

4. In the **Global RADIUS Settings** section, define the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of 5.
5. Define the number of times the SonicWALL security appliance attempts to contact the RADIUS server in the **Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, however 3 RADIUS server retries is recommended.
6. In the **RADIUS Servers** section, specify the settings of the primary RADIUS server in the RADIUS servers section. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.
7. Type the IP address of the RADIUS server in the **IP Address** field.
8. Type the **Port Number** for the RADIUS server.
9. Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
10. If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.

11 Click the **RADIUS Users** tab.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
OK
Cancel
Apply
Help

Privileges for all RADIUS Users

☐ Allow Internet access (when access is restricted)
☐ Bypass filters
☐ Access to VPNs
☐ Access from VPN client with XAUTH
☐ Access from L2TP VPN client.
☐ Limited management capabilities

Ready

12 Select the default privileges for all RADIUS users in this section.

Access to the Internet (when access is restricted) - If you have selected **Allow only authenticated users to access the Internet**, you can allow individual users to access the Internet.

Bypass Filters - Enable this feature if the user has unlimited access to the Internet from the LAN, bypassing SonicWALL security appliance Web, News, Java, and ActiveX blocking.

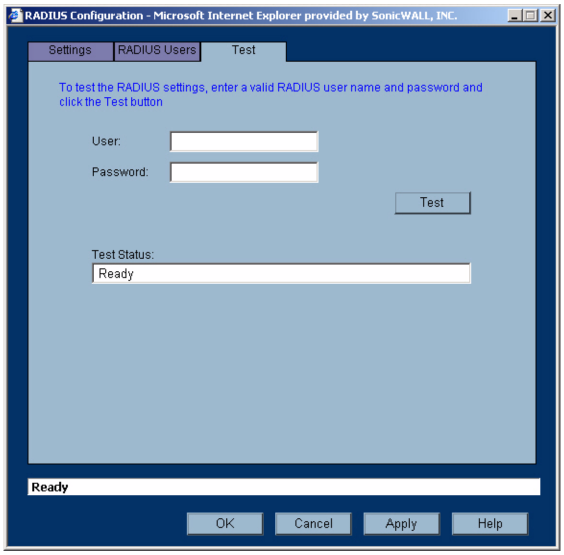
Access to VPNs - Enable feature to allow the user to send information over the VPN connection with authentication enforcement.

Access from the VPN Client with XAUTH - Enable this feature if the user requires XAUTH for authentication and accesses the SonicWALL security appliance via a VPN client.

Access from L2TP VPN client - Enable this feature to allow the user to send information using a L2TP VPN Client with authentication enforcement.

Limited Management Capabilities - Enabling this feature allows the user to have limited local management access to the SonicWALL security appliance Management Interface. This access is limited to the following pages: **General** (Status, Network, Time); **Log** (View Log, Log Settings, Log Reports); **Diagnostics** (All tools except Tech Support Report).

13 Click **Apply**, then click the **Test** tab.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
Test
OK
Cancel
Apply
Help

To test the RADIUS settings, enter a valid RADIUS user name and password and click the Test button

User:

Password:

Test Status:

Ready

Ready

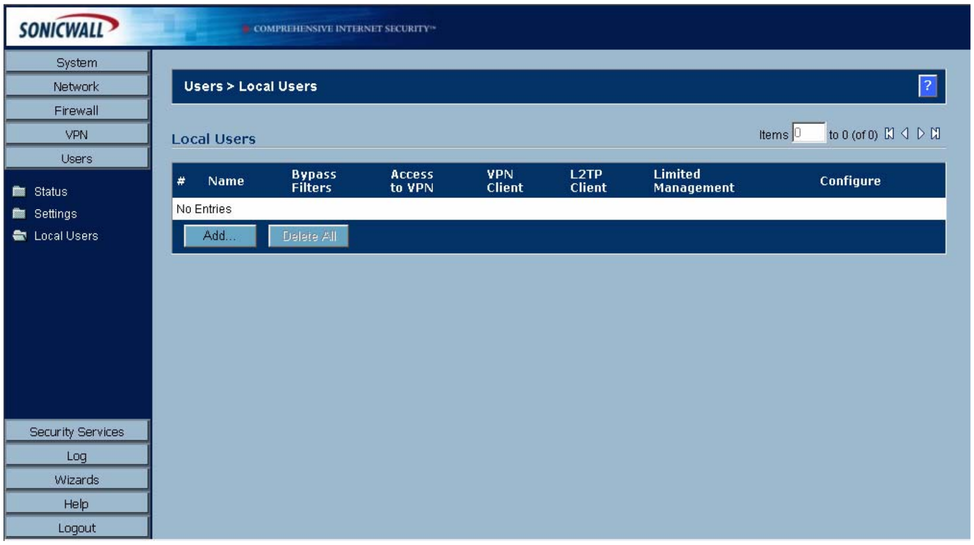
14. Type in a valid user name in the **User** field, and the password in the **Password** field.
15. Click **Test**. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.
16. Click **OK**.

Once the SonicWALL security appliance has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialogue box.

CHAPTER 42

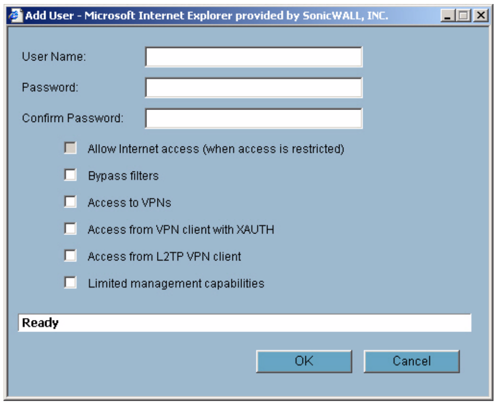
Configuring Local Users

Users > Local Users


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Status
Settings
Local Users
Security Services
Log
Wizards
Help
Logout
Users > Local Users
?
Local Users
Items 0 to 0 (of 0)
Add...
Delete All

#	Name	Bypass Filters	Access to VPN	VPN Client	L2TP Client	Limited Management	Configure
No Entries							

Add local users to the SonicWALL security appliance internal database. Click **Add User** to display the **Add User** configuration window.


Add User - Microsoft Internet Explorer provided by SonicWALL, INC.
OK
Cancel

User Name:

Password:

Confirm Password:

☐ Allow Internet access (when access is restricted)
☐ Bypass filters
☐ Access to VPNs
☐ Access from VPN client with XAUTH
☐ Access from L2TP VPN client
☐ Limited management capabilities

Ready

Adding a Local User

1. Create a user name and type it in the **User Name** field.
2. Create a password for the user and type it in the **Password** field. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.
3. Confirm the password by retyping it in the **Confirm Password** field.
4. Select from the following list of privileges to assign the user:

   Access to the Internet (when access is restricted) - If you have selected **Allow only authenticated users to access the Internet**, you can allow individual users to access the Internet.

   Bypass Filters - Enable this feature if the user has unlimited access to the Internet from the LAN, bypassing SonicWALL security appliance Web, News, Java, and ActiveX blocking.

   Access to VPNs - Enable feature to allow the user to send information over the VPN connection with authentication enforcement.

   Access from the VPN Client with XAUTH - Enable this feature if the user requires XAUTH for authentication and accesses the SonicWALL security appliance via a VPN client.

   Access from L2TP VPN client - Enable this feature to allow the user to send information using a L2TP VPN Client with authentication enforcement.

   Limited Management Capabilities - Enabling this feature allows the user to have limited local management access to the SonicWALL Management Interface. This access is limited to the following pages: **General** (Status, Network, Time); **Log** (View Log, Log Settings, Log Reports); **Modem** (Status, Settings, Failover, Dialup Profiles); **Diagnostics** (All tools except Tech Support Report).
5. Click **OK**.

The users you add appear in the Local Users table with their privileges listed. Click the edit icon in the **Configure** column to edit the user information. Click the delete icon to delete a user.

PART 10

Security Services

CHAPTER

43

Managing SonicWALL Security Services

SonicWALL Security Services

SonicWALL, Inc. offers a variety of subscription-based security services to provide layered security for your network. SonicWALL security services are designed to integrate seamlessly into your network to provide complete protection.

The following security services are listed in **Security Services** in the SonicWALL security appliance’s management interface:

- SonicWALL Content Filtering Service
- SonicWALL Network Anti-Virus/E-Mail Filter
- SonicWALL Gateway Anti-Virus
- SonicWALL Intrusion Prevention Service
- SonicWALL Global Security Client

✓ **Tip:** *After you register your SonicWALL security appliance, you can try FREE TRIAL of these services.*

You can activate and manage SonicWALL security services directly from the SonicWALL management interface or from <https://www.mySonicWALL.com>.

Note: *For more information on SonicWALL security services, please visit <http://www.sonicwall.com>.*

Note: *Complete product documentation for SonicWALL security services are on the SonicWALL security appliance Resource CD or on the SonicWALL documentation site at <http://www.sonicwall.com/services/documentation.html>.*

mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL security appliance
- Try free trials of SonicWALL security services
- Purchase/Activate SonicWALL security service licenses
- Receive SonicWALL firmware and security service updates and alerts
- Manage your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and free. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliances and activate any SonicWALL Security Services associated with the SonicWALL security appliance.

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

Activating Free Trials

You can activate free 30-day trails of the following SonicWALL security services when you register your SonicWALL security appliance at mysonicwall.com:

- SonicWALL Content Filtering Service
- SonicWALL Network Anti-Virus/E-Mail Filter
- SonicWALL Gateway Anti-Virus
- SonicWALL Intrusion Prevention Service

Note: *Refer to Chapter 1, Basic SonicWALL Security Appliance Setup for instructions on registering your SonicWALL security appliance.*

Security Services > Summary

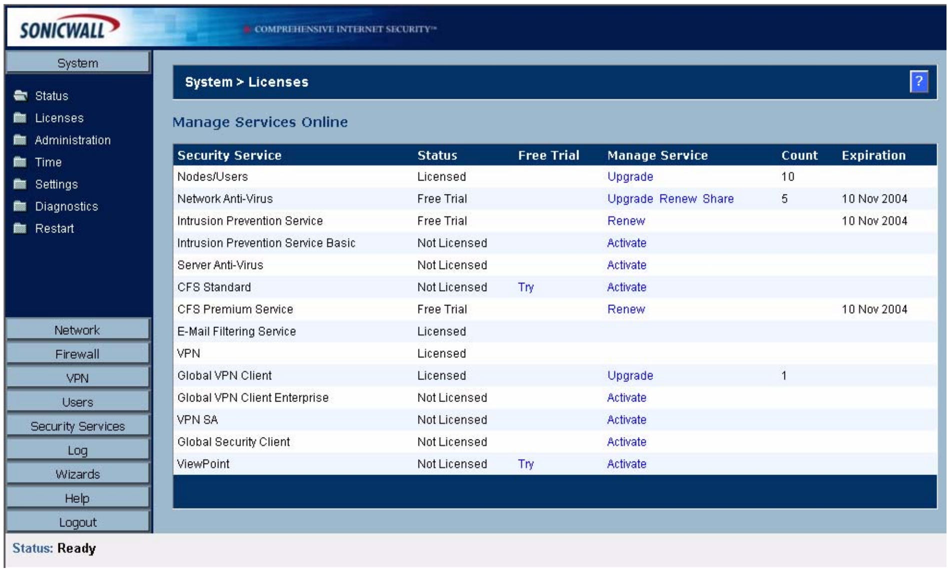
The **Security Services > Summary** page lists the available SonicWALL security services and upgrades available for your SonicWALL security appliance and provides access to mySonicWALL.com to activate services.

Security Services Summary

A list of currently available services through mySonicWALL.com is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. If the service is limited to a number of users, the number is displayed in the **Count** column. The service expiration date is displayed in the **Expiration** column.

Manage Licenses

Clicking the **Manage Licenses** button displays the **mySonicWALL.com Login page** for accessing your mysonicwall.com account licensing information. Enter your mySonicWALL.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System > Licenses** page is displayed with the **Manage Services Online** table. The information in the **Manage Services Online** table is updated from your mysSonicWALL.com account.



System > Licenses

Manage Services Online

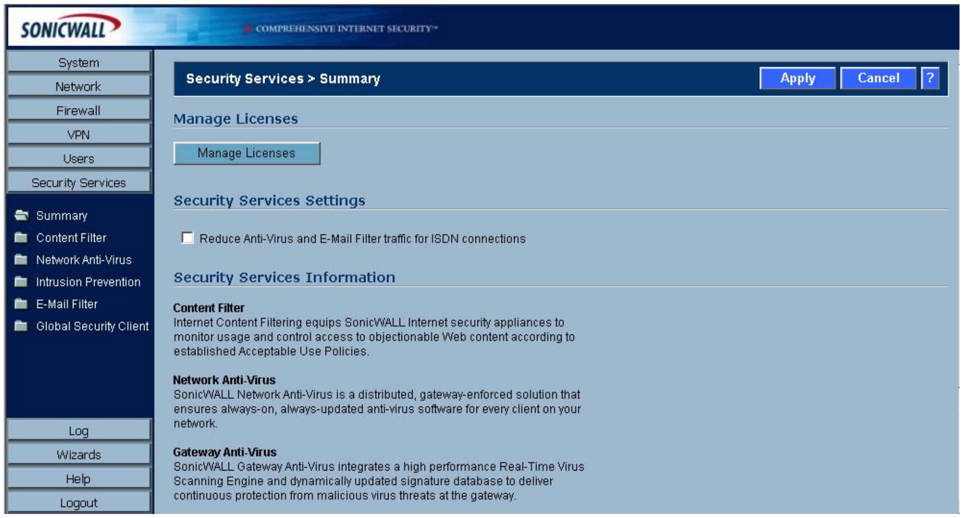
Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed		Upgrade	10	
Network Anti-Virus	Free Trial		Upgrade Renew Share	5	10 Nov 2004
Intrusion Prevention Service	Free Trial		Renew		10 Nov 2004
Intrusion Prevention Service Basic	Not Licensed		Activate		
Server Anti-Virus	Not Licensed		Activate		
CFS Standard	Not Licensed	Try	Activate		
CFS Premium Service	Free Trial		Renew		10 Nov 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	1	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Not Licensed		Activate		
Global Security Client	Not Licensed		Activate		
ViewPoint	Not Licensed	Try	Activate		

Status: **Ready**

If you are already connected to your mysonicwall.com account from the management interface, the **Manage Services Online** table is displayed.

If Your SonicWALL Security Appliance is Not Registered

If your SonicWALL security appliance is not registered, the **Security Services > Summary** page does not include the **Services Summary** table. Your SonicWALL security appliance must be registered to display the **Services Summary** table.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Security Services
Summary
Content Filter
Network Anti-Virus
Intrusion Prevention
E-Mail Filter
Global Security Client
Log
Wizards
Help
Logout
Security Services > Summary
Apply
Cancel
?
Manage Licenses
Manage Licenses
Security Services Settings
Security Services Information

☐ Reduce Anti-Virus and E-Mail Filter traffic for ISDN connections

Content Filter
Internet Content Filtering equips SonicWALL Internet security appliances to monitor usage and control access to objectionable Web content according to established Acceptable Use Policies.

Network Anti-Virus
SonicWALL Network Anti-Virus is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network.

Gateway Anti-Virus
SonicWALL Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.

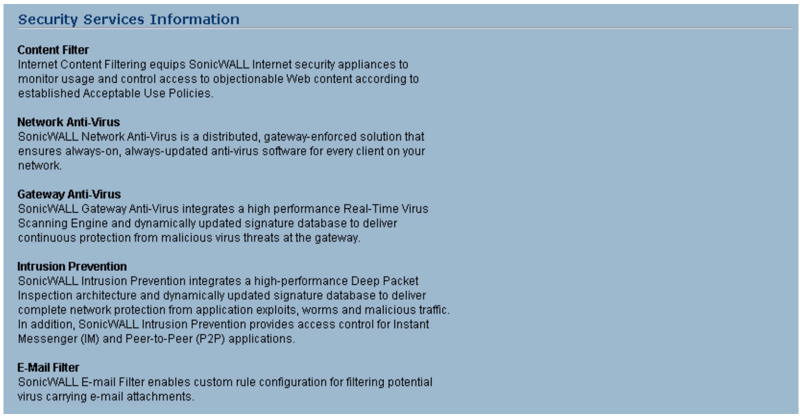
Cross Reference: *Refer to Chapter 2, Basic SonicWALL Security Appliance Setup for instructions on registering your SonicWALL security appliance.*

Security Services Settings

- **Synchronize** - Click **Synchronize** to update the licensing and subscription information on the SonicWALL security appliance from your mysonicwall.com account.
- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an “always on” Internet connection.

Security Services Information

This section includes a brief overview of services available for your SonicWALL security appliance.



Security Services Information

Content Filter
Internet Content Filtering equips SonicWALL Internet security appliances to monitor usage and control access to objectionable Web content according to established Acceptable Use Policies.

Network Anti-Virus
SonicWALL Network Anti-Virus is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network.

Gateway Anti-Virus
SonicWALL Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.

Intrusion Prevention
SonicWALL Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, SonicWALL Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.

E-Mail Filter
SonicWALL E-mail Filter enables custom rule configuration for filtering potential virus carrying e-mail attachments.

CHAPTER

44

Configuring SonicWALL Content Filtering Service

SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries, as well as reduce legal and privacy risks while minimizing administration overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance simple.

SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliances can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

Note: *Refer to the SonicWALL Content Filtering Service Administrator's Guide on the Resource CD or the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html> for complete instructions.*

Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the SonicWALL security appliance Restrict Web Features and Trusted Domains settings, which are included with SonicOS. You can activate and configure SonicWALL Content Filtering Service as well as two third-party Content Filtering products from the **Security Services > Content Filter** page.

Content Filter Status

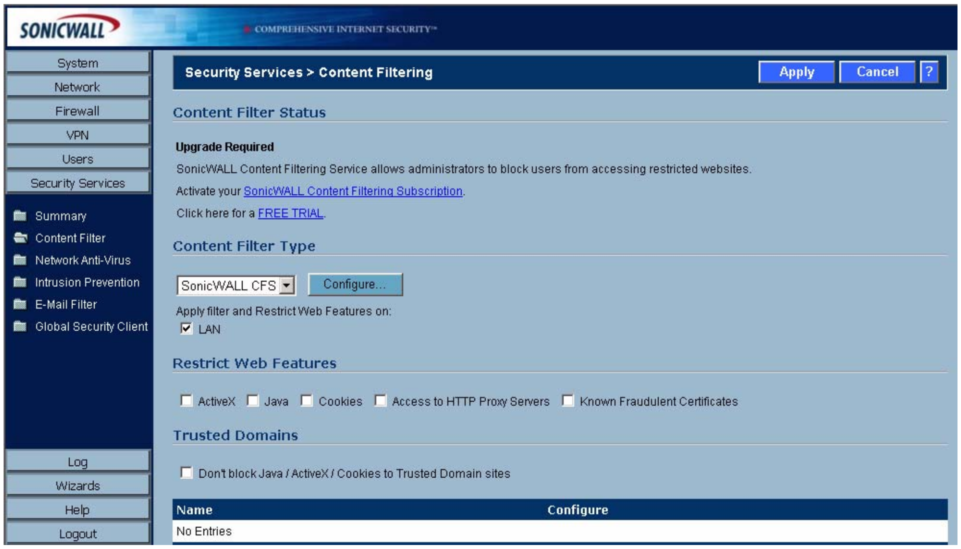
If SonicWALL CFS is activated, the Content Filter Status section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.

You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here**.

If SonicWALL CFS is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

Activating SonicWALL Content Filtering Service

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Users
Security Services
Summary
Content Filter
Network Anti-Virus
Intrusion Prevention
E-Mail Filter
Global Security Client
Log
Wizards
Help
Logout
Apply
Cancel
?

Security Services > Content Filtering

Content Filter Status

Upgrade Required

SonicWALL Content Filtering Service allows administrators to block users from accessing restricted websites.

Activate your SonicWALL Content Filtering Subscription.

Click here for a FREE TRIAL.

Content Filter Type

SonicWALL CFS ▾ Configure...

Apply filter and Restrict Web Features on:

☑ LAN

Restrict Web Features

☐ ActiveX ☐ Java ☐ Cookies ☐ Access to HTTP Proxy Servers ☐ Known Fraudulent Certificates

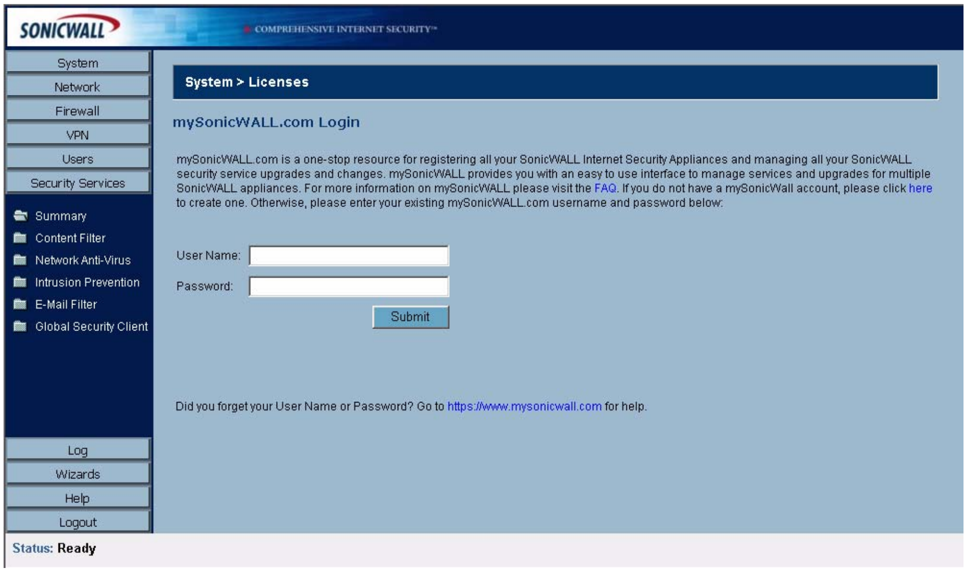
Trusted Domains

☐ Don't block Java / ActiveX / Cookies to Trusted Domain sites

Name	Configure
No Entries	

Alert: *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1 Click the **SonicWALL Content Filtering Subscription** link on the Security **Services > Content Filtering** page. The **mySonicWALL.com Login** page is displayed.



System > Licenses

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:
Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

Status: Ready

2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.

3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL security appliance.

If you activated SonicWALL CFS at mySonicWALL.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

Activating a SonicWALL Content Filtering Service FREE TRIAL

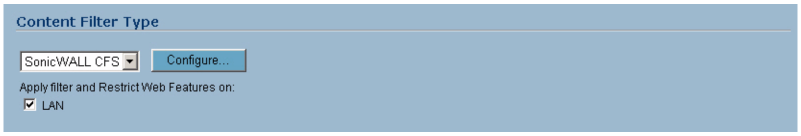
You can try a FREE TRIAL of SonicWALL CFS by following these steps:

1 Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.

2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.

3 Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL security appliance.

Content Filter Type


Content Filter Type

SonicWALL CFS

Apply filter and Restrict Web Features on:

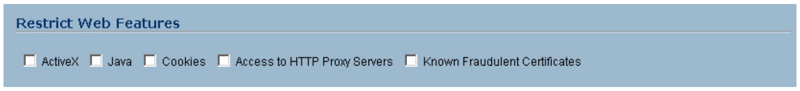
☑ LAN

There are three types of content filtering available on the SonicWALL security appliance.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to use the SonicWALL Content Filtering Service that is available as an upgrade. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html>
- **N2H2** - N2H2 is a third party content filter software package supported by SonicWALL security appliance.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWALL security appliance.

Apply filter and Restrict Web Features on - Allows you to specify the **LAN** interface for applying content filtering or **Restrict Web Features** protection.

Restrict Web Features


Restrict Web Features

☐ ActiveX ☐ Java ☐ Cookies ☐ Access to HTTP Proxy Servers ☐ Known Fraudulent Certificates

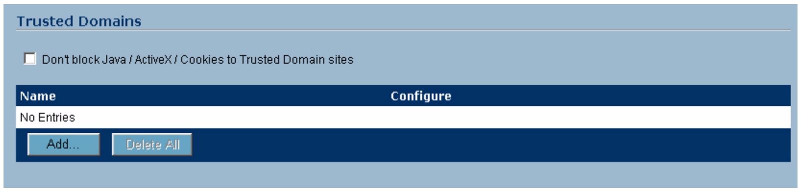
Restrict Web Features enhances your network security by blocking potentially harmful Web applications from entering your network.

Restrict Web Features are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL security appliance blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL security appliance include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

You can choose **LAN** for applying your **Restrict Web Features** protection from the **Apply filter and Restrict Web Features on** setting in Content Filter Type.

Trusted Domains



☐ Don't block Java / ActiveX / Cookies to Trusted Domain sites

Name	Configure
No Entries	

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features.** If you trust content on specific domains and want them exempt from **Restrict Web Features**, follow these steps to add them

1. Select **Don't block Java/ActiveX/Cookies to Trusted Domain sites**.
2. Click **Add**. The **Add Trusted Domain Entry** window is displayed.
3. Enter the trusted domain name in the **Domain Name** field.
4. Click **OK**. The trusted domain entry is added to the Trusted Domain table.

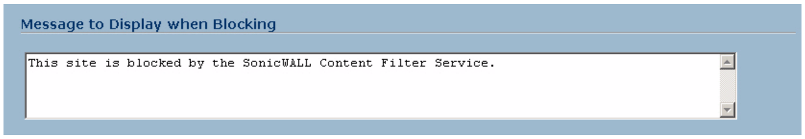
To keep the trusted domain entries but enable Restrict Web Features, uncheck **Don't block Java/ ActiveX/Cookies to Trusted Domains**.

To delete an individual trusted domain, click on the delete 🗑 icon for the entry.

To delete all trusted domains, click the **Delete All** button

To edit a trusted domain entry, click the edit ✎ icon.

Message to Display when Blocking



This site is blocked by the SonicWALL Content Filter Service.

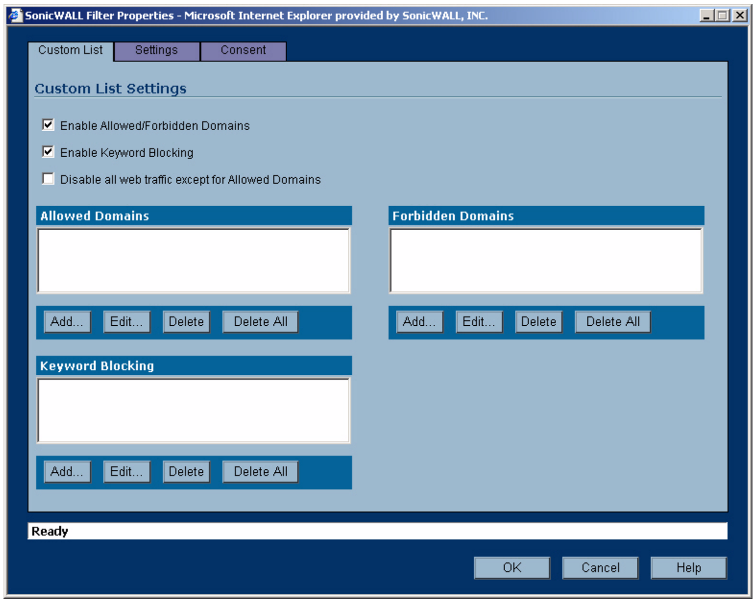
You can enter your customized text to display to the user when access to a blocked site is attempted. The default message is **This site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.

Configuring SonicWALL Filter Properties

You can customize SonicWALL security appliance filter features included with SonicOS Standard from the **SonicWALL Filter Properties** window. To display the **SonicWALL Filter Properties** window, select **SonicWALL CFS** from the **Content Filter Type** menu on the **Security Services > Content Filter** page, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.

Note: *If SonicWALL Premium Content Filtering Service is activated, the SonicWALL Filter Properties window includes additional configuration pages:* ***CFS*** *and* ***URL List****. Refer to the SonicWALL Premium Content Filtering Service Administrator's Guide on the Resource CD or the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html> for complete instructions.*

Custom List


SonicWALL Filter Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
Custom List
Settings
Consent
Custom List Settings
Allowed Domains
Forbidden Domains
Keyword Blocking
Add...
Edit...
Delete
Delete All
Ready
OK
Cancel
Help

☑ Enable Allowed/Forbidden Domains
☑ Enable Keyword Blocking
☐ Disable all web traffic except for Allowed Domains

The **Custom List** page allows you to specify allowed or forbidden domains and keywords to block.

Allowed/Forbidden Domains

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. Select the check box **Enable Allowed/Forbidden Domains** to activate this feature.

To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.

Alert: *Do not include the prefix “http://” in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”.*

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

Keyword Blocking

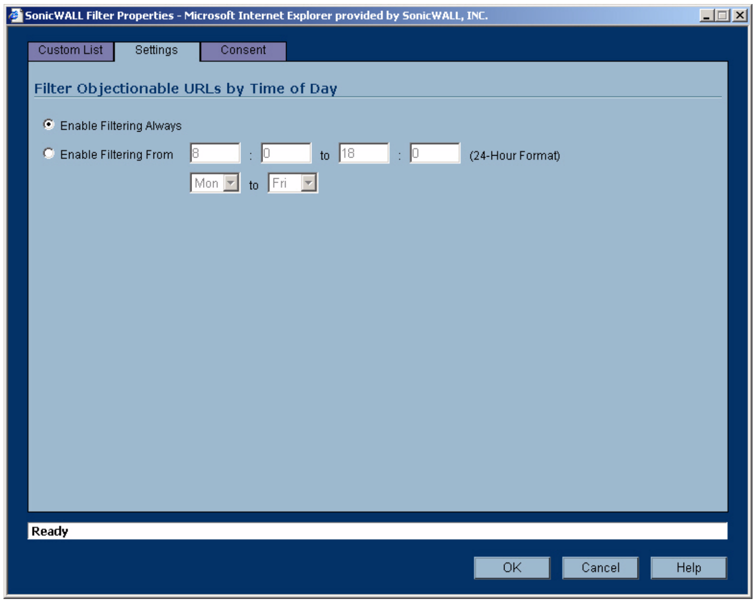
To enable blocking using **Keywords**, select **Enable Keyword Blocking**.Click **Add**, and enter the keyword to block in the **Add Keyword** field, and click **OK**.

To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

Disable all Web traffic except for Allowed Domains

When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL security appliance only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

Settings


SonicWALL Filter Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
Custom List
Settings
Consent
OK
Cancel
Help

Filter Objectionable URLs by Time of Day

● Enable Filtering Always

○ Enable Filtering From 8 : 0 to 18 : 0 (24-Hour Format)

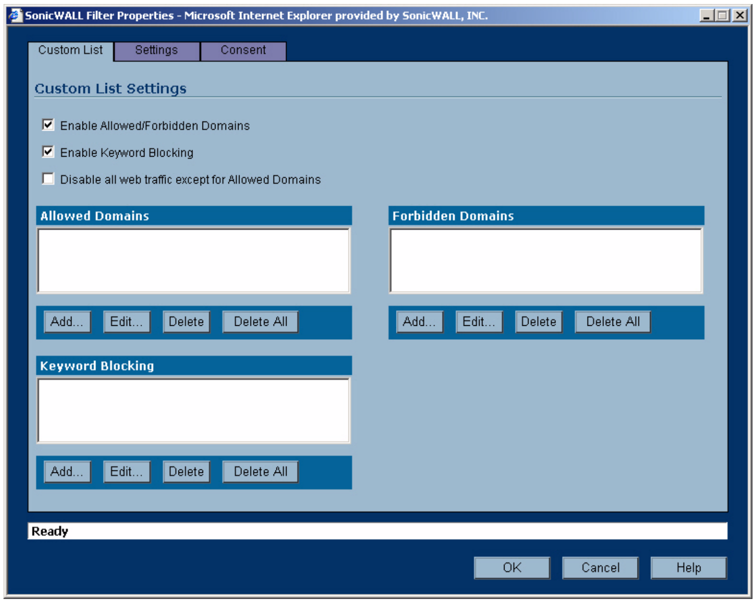
Mon to Fri

Ready

The **Settings** page allows you specify time periods for enabling the filtering of objectionable URLs specified in the **Custom List** page. For example, you could configure the SonicWALL security appliance to filter employee Internet access during normal business hours, but allow unrestricted access at night and on weekends.

- **Enable Filtering Always** - When selected, filtering is enforced at all times.
- **Enable Filtering From** - When selected, filtering is enforced during the time and days specified. Enter the time period, in 24-hour format in the hour and minute fields, and select the start and end days of the week from the menus.

Consent



Custom List Settings

☑ Enable Allowed/Forbidden Domains

☑ Enable Keyword Blocking

☐ Disable all web traffic except for Allowed Domains

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.

To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes) -** In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL security appliance can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWALL security appliance requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL security appliance, which, when selected, tell the SonicWALL security appliance if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL security appliance LAN IP Address is used instead of 192.168.168.168"\.
- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

Mandatory Filtered IP Addresses

Consent Page URL (mandatory filtering)

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL security appliance that tells the SonicWALL security appliance that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL security appliance LAN IP Address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

Adding a New Address

The SonicWALL security appliance can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window.

Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete.**

CHAPTER

45

Managing SonicWALL Network Anti-Virus and E-Mail Filter Services

SonicWALL Network Anti-Virus Overview

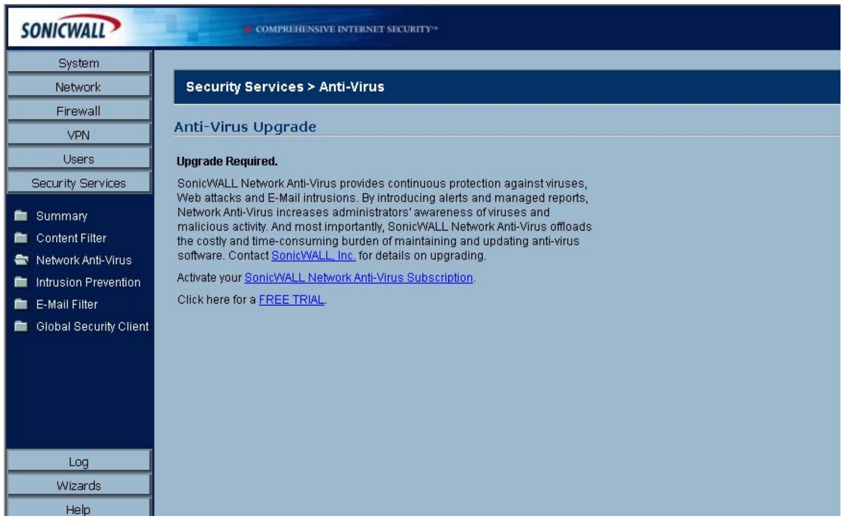
The widespread outbreaks of viruses illustrate the problematic nature of virus defense for small offices. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time.

SonicWALL Network Anti-Virus is a SonicWALL subscription service that prevents occurrences like these and offers a new approach to virus protection. The SonicWALL security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL security appliance restricts network users' access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

Note: *Refer to the SonicWALL Network Anti-Virus Administrator's Guide available at the SonicWALL documentation Web site <http://www.sonicwall.com/services/documentation.html> for complete configuration instructions.*

Security Services > Anti-Virus

If SonicWALL Network Anti-Virus is not activated, the **Security Services > Anti-Virus** page indicates an upgrade is required and provides links to activate a SonicWALL CFS license or activate a free trial version.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Security Services
Summary
Content Filter
Network Anti-Virus
Intrusion Prevention
E-Mail Filter
Global Security Client
Log
Wizards
Help

Security Services > Anti-Virus

Anti-Virus Upgrade

Upgrade Required.

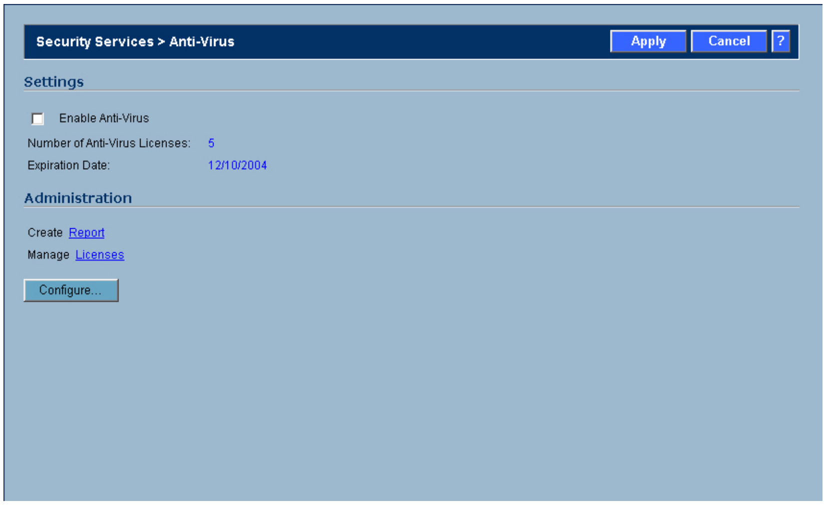
SonicWALL Network Anti-Virus provides continuous protection against viruses, Web attacks and E-Mail intrusions. By introducing alerts and managed reports, Network Anti-Virus increases administrators' awareness of viruses and malicious activity. And most importantly, SonicWALL Network Anti-Virus offloads the costly and time-consuming burden of maintaining and updating anti-virus software. Contact SonicWALL, Inc. for details on upgrading.

Activate your SonicWALL Network Anti-Virus Subscription.

Click here for a FREE TRIAL.

If you do not have an Activation Key, you must purchase SonicWALL Network Anti-Virus from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada). If you have an Activation Key, you can activate SonicWALL Network Anti-Virus from this page.

If SonicWALL Network Anti-Virus is activated on your SonicWALL security appliance, the **Security Services > Anti-Virus** page includes status information and access to configuration settings.


Apply
Cancel
?
Configure...

Security Services > Anti-Virus

Settings

☐ Enable Anti-Virus

Number of Anti-Virus Licenses: 5

Expiration Date: 12/10/2004

Administration

Create Report

Manage Licenses

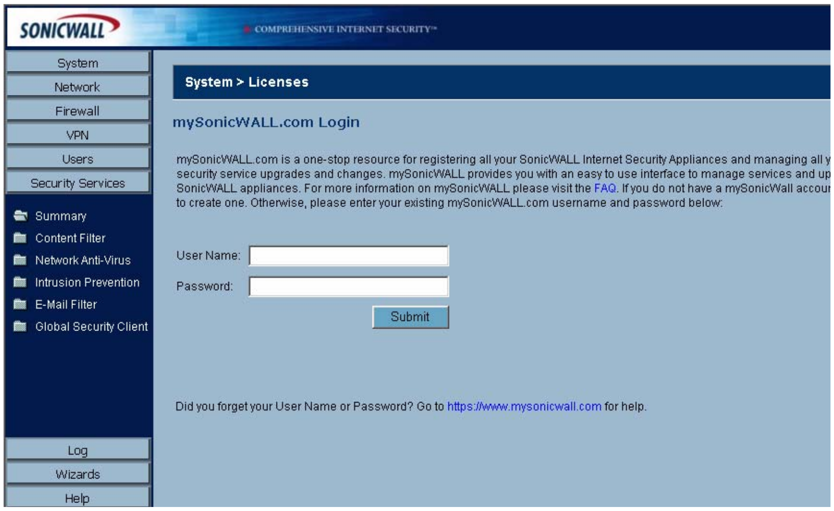
Note: *Refer to the SonicWALL Network Anti-Virus Administrator's Guide on the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html> for complete instructions on setting up Network Anti-Virus on your SonicWALL security appliance.*

Activating SonicWALL Network Anti-Virus

If you have an Activation Key for your SonicWALL Network Anti-Virus subscription, follow these steps to activate SonicWALL Network Anti-Virus:

Alert: *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1 Click the **SonicWALL Network Anti-Virus Subscription** link on the **Security Services > Anti-Virus** page. The **mySonicWALL.com Login** page is displayed.



mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all y
security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and up
SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall accour
to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Network Anti-Virus Subscription** link.

3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL security appliance.

If you activated SonicWALL Network Anti-Virus at www.mySonicWALL.com, the SonicWALL Network Anti-Virus activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

Activating a SonicWALL Network Anti-Virus FREE TRIAL

You can try a FREE TRIAL of SonicWALL Network Anti-Virus by following these steps:

Alert: *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1 Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.

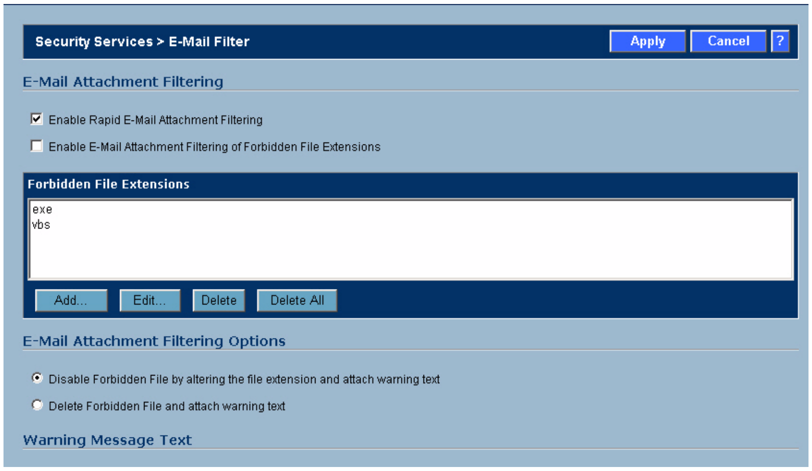
2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.

3 Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL.

Security Services > E-Mail Filter

The **Security Services > E-Mail Filter** page allows the administrator to selectively delete or disable inbound e-mail attachments as they pass through the SonicWALL security appliance. This feature provides control over executable files and scripts, and applications sent as e-mail attachments.

E-Mail Filter is included with SonicWALL Network Anti-Virus. When you activate Network Anti-Virus, the settings on the **Security Services > E-Mail Filter** page are displayed.



E-Mail Attachment Filtering

☑ Enable Rapid E-Mail Attachment Filtering

☐ Enable E-Mail Attachment Filtering of Forbidden File Extensions

Forbidden File Extensions

exe
vbs

E-Mail Attachment Filtering Options

● Disable Forbidden File by altering the file extension and attach warning text

○ Delete Forbidden File and attach warning text

Warning Message Text

Configuring SonicWALL Network Anti-Virus

If you have activated a SonicWALL Network Anti-Virus license or FREE TRIAL version, refer to the *SonicWALL Content Filtering Service Administrator's Guide* available at the SonicWALL documentation Web site <http://www.sonicwall.com/services/documentation.html> for complete configuration instructions.

CHAPTER

46

Managing SonicWALL Gateway Anti-Virus Service

SonicWALL Gateway Anti-Virus Overview

SonicWALL Gateway Anti-Virus is part of the SonicWALL Gateway Anti-Virus/Intrusion Prevention Service solution that provides comprehensive protection against real-time for viruses, worms, Trojans, and software vulnerabilities using deep packet inspection scanning engine. SonicWALL's unique solution features a high-performance deep packet inspection architecture that scans for viruses on a packet-by-packet basis, rather than copy every packet into a file and then scanning the file. SonicWALL Gateway Anti-Virus has the capacity to analyze files of any size and an unlimited number of files per user, providing ultimate scalability.

When you activate SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service is also activated to provide comprehensive, real-time gateway anti-virus and intrusion prevention. The SonicWALL Gateway Anti-Virus/Intrusion Prevention Services secures your network from the gateway against a comprehensive array of dynamic threats. No client software is required.

Note: *Refer to the SonicWALL Intrusion Prevention Service 2.0 Administrator's Guide for information you need to successfully activate, configure, and administer SonicWALL Intrusion Prevention Service 2.0 on a SonicWALL security appliance.*

SonicWALL Gateway Anti-Virus delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of high threat virus signatures. Virus attacks are caught and suppressed before they travel to employee desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

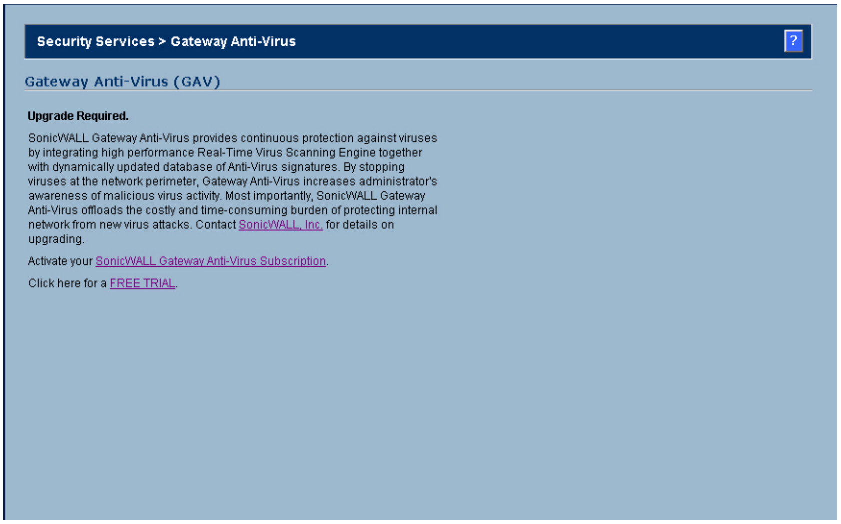
SonicWALL Gateway Anti-Virus can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL Gateway Anti-Virus integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

SonicWALL Gateway Anti-Virus/Intrusion Prevention Features

- **Real-Time Anti-Virus Gateway Scanning** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service delivers intelligent file-based virus and malicious code prevention through a patent-pending deep packet inspection virus scanning engine that scans for viruses, worms and other Internet threats in real-time over the corporate network.
- **Powerful Intrusion Prevention** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides complete protection from a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.
- **Integrated Deep Packet Inspection Technology** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service features a patent-pending, high-performance deep packet inspection engine that uses parallel searching algorithms up through the application layer to deliver increased application layer, Web and e-mail, attack prevention capabilities over those supplied by traditional stateful packet inspection firewalls. Parallel processing reduces the performance impact on the firewall and maximizes available memory for exceptional throughput on SonicWALL security appliance.
- **Inter-zone Anti-Virus Scanning** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides an additional layer of protection against malicious threats by allowing administrators to enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones (SonicOS Enhanced)
- **Extensive Virus Signature List** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service utilizes an extensive database containing thousands of attack and vulnerability signatures written to detect and prevent intrusions, viruses, worms, application exploits, and the use of peer-to-peer and instant messaging applications.
- **Application Control** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service provides network administrator’s with the ability to monitor and manage the use of instant messaging and peer-to-peer file sharing programs from operating through the firewall, closing a potential backdoor that can be used to compromise the network while improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL Gateway Anti-Virus/Intrusion Prevention Service allows network administrators to create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.

Activating SonicWALL Gateway Anti-Virus

If you do not have SonicWALL Gateway Anti-Virus installed on your SonicWALL security appliance, the **Security Services > Gateway Anti-Virus** page indicates an upgrade is required and includes a link to activiate it from your SonicWALL security appliance management interface.



Gateway Anti-Virus (GAV)

Upgrade Required.

SonicWALL Gateway Anti-Virus provides continuous protection against viruses by integrating high performance Real-Time Virus Scanning Engine together with dynamically updated database of Anti-Virus signatures. By stopping viruses at the network perimeter, Gateway Anti-Virus increases administrator's awareness of malicious virus activity. Most importantly, SonicWALL Gateway Anti-Virus offloads the costly and time-consuming burden of protecting internal network from new virus attacks. Contact SonicWALL, Inc. for details on upgrading.

Activate your SonicWALL Gateway Anti-Virus Subscription.

Click here for a FREE TRIAL.

If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus or activate a SonicWALL Gateway Anti-Virus license directly from the SonicWALL management interface. If you need to create a mySonicWALL.com account to register your SonicWALL security appliance, you can create it directly from the SonicWALL management interface.

SonicWALL Gateway Anti-Virus is part of the unified SonicWALL Gateway Anti-Virus/Intrusion Prevention Service that provides comprehensive protection against viruses, worms, Trojans, and other vulnerabilities. When you activate SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service is also activated.

Note: *Refer to the SonicWALL Intrusion Prevention Service 2.0 Administrator's Guide for the information you need to successfully activate, configure, and administer SonicWALL Intrusion Prevention Service 2.0 on a SonicWALL security appliance.*

Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.

If you do not have a SonicWALL Gateway Anti-Virus license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you activated SonicWALL Gateway Anti-Virus at <https://www.mysonicwall.com>, SonicWALL Gateway Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

mySonicWALL.com registration information is not sold or shared with any other company.

Activating SonicWALL Gateway Anti-Virus

If you have an Activation Key for your SonicWALL Gateway Anti-Virus, perform these steps to activate the service:

1. On the **Security Services > Gateway Anti-Virus** page, click the **SonicWALL Gateway Anti-Virus Subscription** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
4. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Gateway Anti-Virus subscription is activated on your SonicWALL security appliance.

If you activated the SonicWALL Gateway Anti-Virus subscription on mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

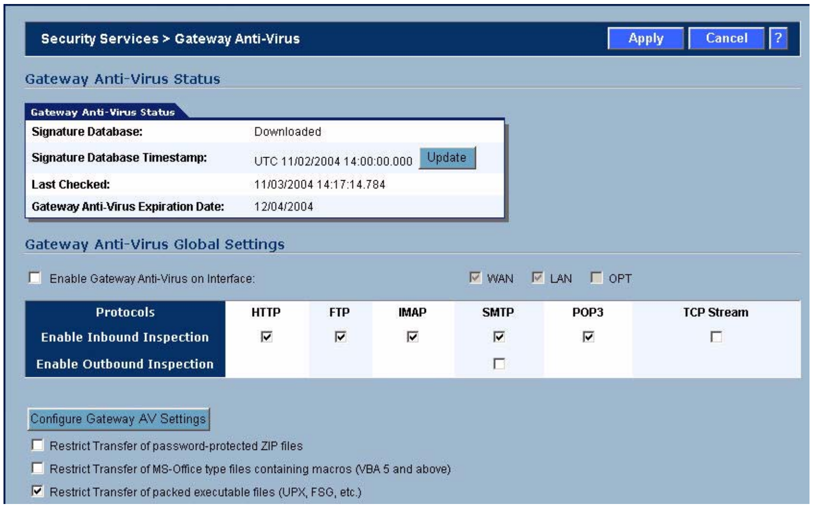
Activating the SonicWALL Gateway Anti-Virus FREE TRIAL

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, perform these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. Your SonicWALL Gateway Anti-Virus trial subscription is activated on your SonicWALL security appliance.

Configuring SonicWALL Gateway Anti-Virus

After activating SonicWALL Gateway Anti-Virus, the **Security Services > Gateway Anti-Virus** page displays the configuration settings for managing the service on your SonicWALL security appliance.


Security Services > Gateway Anti-Virus
Apply
Cancel
?
Update
Configure Gateway AV Settings

Gateway Anti-Virus Status

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 11/02/2004 14:00:00.000
Last Checked:	11/03/2004 14:17:14.784
Gateway Anti-Virus Expiration Date:	12/04/2004

Gateway Anti-Virus Global Settings

☐ Enable Gateway Anti-Virus on Interface: ☑ WAN ☑ LAN ☐ OPT

Protocols	HTTP	FTP	IMAP	SMTP	POP3	TCP Stream
Enable Inbound Inspection	☑	☑	☑	☑	☑	☐
Enable Outbound Inspection				☐		

☐ Restrict Transfer of password-protected ZIP files
☐ Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)
☑ Restrict Transfer of packed executable files (UPX, FSG, etc.)

If you have activated a SonicWALL Content Filtering Service license or FREE TRIAL version, refer to the SonicWALL Gateway Anti-Virus Administrator’s Guide available at the SonicWALL documentation Web site <http://www.sonicwall.com/services/documentation.html> for complete configuration instructions.

CHAPTER 47

Managing SonicWALL Intrusion Prevention Service

SonicWALL Intrusion Prevention Service

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Note: *Refer to the SonicWALL Intrusion Prevention Service Administrator's Guide on the Resource CD or the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html> for complete instructions.*

SonicWALL IPS Features

- **High Performance Deep Packet Inspection Technology** - SonicWALL's Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection engine that uses parallel searching algorithms on incoming packets through the application layer to deliver increased attack prevention capabilities over those supplied by traditional stateful packet inspection firewall. By performing all of the matching on packets, SonicWALL IPS eliminates the overhead of having to reassemble the data stream. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL security appliances.
- **Inter-Zone Intrusion Prevention** - SonicWALL IPS provides an additional layer of protection against malicious threats by allowing administrator's to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones. This is performed by enabling intrusion prevention on inbound and outbound traffic between trusted zones (SonicOS Enhanced).
- **Extensive Signature Database** - SonicWALL IPS utilizes an extensive database of over 1,700 attack and vulnerability signatures written to detect and prevent intrusions, worms, application exploits, as well as peer-to-peer and instant messaging traffic. The SonicWALL Deep Packet Inspection engine can also read signatures written in the popular Snort format, allowing SonicWALL to easily incorporate new signatures as they are published by third parties. SonicWALL

maintains a current and robust signature database by incorporating the latest available signatures from thousands of open source developers and by continually developing new signatures for application vulnerabilities that are not immediately available or provided by open source.

- **Dynamically Updated Signature Database** - SonicWALL IPS includes automatic signature updates delivered through SonicWALL's Distributed Enforcement Architecture (DEA), providing protection from emerging threats and lowering total cost of ownership. Updates to the signature database are dynamic for SonicWALL security appliances under an active subscription.
- **Scalable** - SonicWALL IPS is a scalable solution for SonicWALL TZ and PRO Series Appliances that secures small, medium and large networks with complete protection from application exploits, worms and malicious traffic.
- **Application Control** - SonicWALL IPS provides the ability to prevent Instant Messaging and Peer-to-Peer file sharing programs from operating through the firewall, closing a potential backdoor that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL IPS allows network administrators to quickly and easily manage the service within minutes. Administrator's can create global policies between security zones and interfaces as well as group attacks by priority, simplifying deployment and management across a distributed network.
- **Granular Policy Management -** SonicWALL IPS provides administrators with a range of granular policy tools to enforce IPS on a global, group, or individual signature level to enable more control and reduce the number of false policies. SonicWALL IPS allows also allows administrators to choose between detection, prevention, or both to tailor policies for their specific network environment.
- **Logging and Reporting** - SonicWALL IPS offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrator's to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System. A hyperlink of the intrusion brings up the signature window for further information from the SonicWALL security appliance log.
- **Management by Risk Category** - SonicWALL IPS allows you to enable/disable detection or prevention based on the priority level of attack through High, Medium, or Low predefined priority groups.
- **Detection Accuracy** - SonicWALL IPS detection and prevention accuracy is achieved minimizing both false positives and false negatives. Signatures are written around applications, such as Internet Explorer or SQL Server rather than ports or protocols to ensure that malicious code targeting them are correctly identified and prevented.

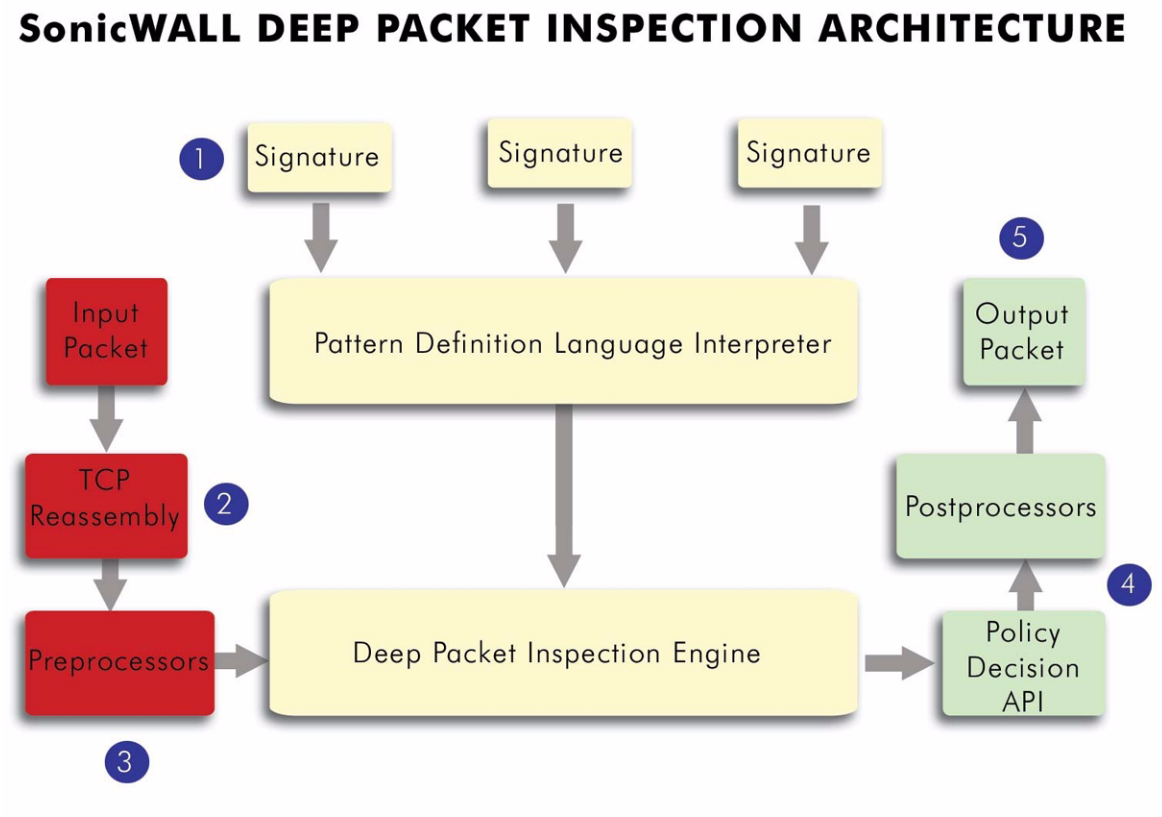
SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWALL security appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL security appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

How SonicWALL's Deep Packet Inspection Architecture Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.


SonicWALL DEEP PACKET INSPECTION ARCHITECTURE
1
Signature
Signature
Signature
5
Input Packet
Pattern Definition Language Interpreter
Output Packet
TCP Reassembly
2
Postprocessors
4
Preprocessors
Deep Packet Inspection Engine
Policy Decision API
3

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
5. SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

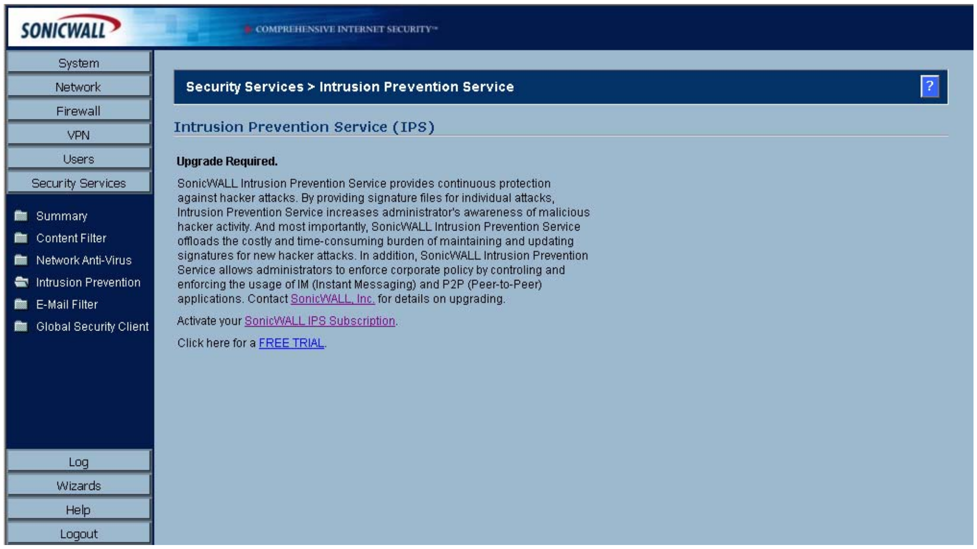
Security Services > Intrusion Prevention

The **Security Services > Intrusion Prevention** page provides the settings for configuring SonicWALL Intrusion Prevention Service.

If you do not have SonicWALL IPS activated on your SonicWALL security appliance, you must purchase SonicWALL IPS from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you do not have SonicWALL IPS installed on your SonicWALL security appliance, the **Security Services > Intrusion Prevention** page indicates an upgrade is required and includes a link to activate your IPS subscription from the SonicWALL management interface or to activate a FREE TRIAL of SonicWALL IPS.

Activating SonicWALL IPS



Intrusion Prevention Service (IPS)

Upgrade Required.

SonicWALL Intrusion Prevention Service provides continuous protection against hacker attacks. By providing signature files for individual attacks, Intrusion Prevention Service increases administrator's awareness of malicious hacker activity. And most importantly, SonicWALL Intrusion Prevention Service offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks. In addition, SonicWALL Intrusion Prevention Service allows administrators to enforce corporate policy by controling and enforcing the usage of IM (Instant Messaging) and P2P (Peer-to-Peer) applications. Contact SonicWALL, Inc. for details on upgrading.

Activate your SonicWALL IPS Subscription.

Click here for a FREE TRIAL.

If you have an Activation Key for your SonicWALL IPS, follow these steps to activate the service:

1. Click the **SonicWALL IPS Subscription** link on the **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL IPS Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL IPS subscription is activated on your SonicWALL security appliance.

If you activated the SonicWALL IPS subscription on mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

Activating the SonicWALL IPS FREE TRIAL

To try a FREE TRIAL of SonicWALL IPS, follow these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL IPS trial subscription is activated on your SonicWALL security appliance.

CHAPTER

48

Managing SonicWALL Global Security Client

SonicWALL Global Security Client

The SonicWALL Global Security Client combines gateway enforcement, central management, configuration flexibility and software deployment to deliver comprehensive desktop security for remote/mobile workers and corporate networks. It offers administrators the capability to manage a mobile/remote user's online access, based on corporate policies, to ensure optimal security of the network and maximize network resources. Instant messaging, high-risk Web sites and network file access can all be allowed or disallowed as security and productivity concerns dictate. Different remote/mobile users can be organized into adaptable groups with differing policies at a granular level.

SonicWALL Global Security Client delivers a low-maintenance solution to allow network administrators to secure mobile users. Residing on the remote user's system, the Global Security Client automatically communicates with an organization's SonicWALL gateway back at the office when an individual logs in to the network. Prior to allowing network access, the gateway administrator automatically updates the Global Security Client with the latest security policies and software updates. No prompting or intervention is necessary by the administrator or the remote user - it's completely seamless and transparent.

Global Security Client protection includes the SonicWALL Distributed Security Client and the SonicWALL Global VPN Client combined with centrally managed security policies via the SonicWALL Internet Security Appliance and SonicWALL's industry-leading Distributed Enforcement Architecture (DEA).

Note: *Refer to the SonicWALL Global Security Client Administrator's Guide on the Resource CD or the SonicWALL documentation Web site at <http://www.sonicwall.com/services/documentation.html> for complete instructions on this service.*

Global Security Client Features

- **Multi-Pronged Protection** - extends the boundaries of security by protecting the corporate network and remote/mobile workers from malicious attacks that occur over the Internet.
- **Enhanced Application Security** - provides an additional layer of security by protecting organizations against legal liabilities that occur when employees accidentally or intentionally run applications from the Internet that have been designated as “untrusted” by the network administrator.
- **Policy Management** - enables network administrator’s to create, distribute and manage global security policies for remote and mobile users from a central location. Once a new policy is created, it is seamlessly distributed to every system on the network with no end-user interaction required. Configuration options include specifying the minimum application version, policy levels and behavior for clients not in compliance.
- **Gateway Enforcement** - enforces security policies at the gateway to ensure the end-user’s system is in compliance before being granted access to the network. Users without the Global Security Client installed on their systems must contact their administrator.
- **Scalable Architecture** - features a unique client/gateway enforcement architecture that delivers comprehensive security, scaling from the individual telecommuters and mobile users up to larger, more diverse deployments with a worldwide mobile workforce.
- **Low Total Cost of Ownership** - addresses the needs of organizations looking to deploy comprehensive desktop security to remote/mobile workers and corporate networks while delivering a lower total cost of ownership through automated policy enforcement and software distribution at the gateway.
- **Easy-to-Use Local Interface** - includes an intuitive user interface that seamlessly integrates multiple applications and presents the administrator with a status page and optional configuration functionality, offering enhanced ease of use.
- **Application Reporting** - includes application reporting to provide network administrators with data on the status of the application, as well as the ability to monitor for unusual activities and perform troubleshooting.

How SonicWALL Global Security Client Works

The security administrator logs into the SonicWALL gateway to create security policies for all Global Security Clients using the intuitive Policy Editor interface. The Policy Editor allows the security administrator to create, edit, and deploy security policies that are automatically enforced by the SonicWALL gateway. When a remote user logs into the corporate network using the Global VPN Client Enterprise, the SonicWALL gateway seamlessly updates the user’s security policy for the Distributed Security Client to ensure the client is in full compliance with corporate security policies while establishing a secure VPN connection via the Global VPN Client Enterprise.

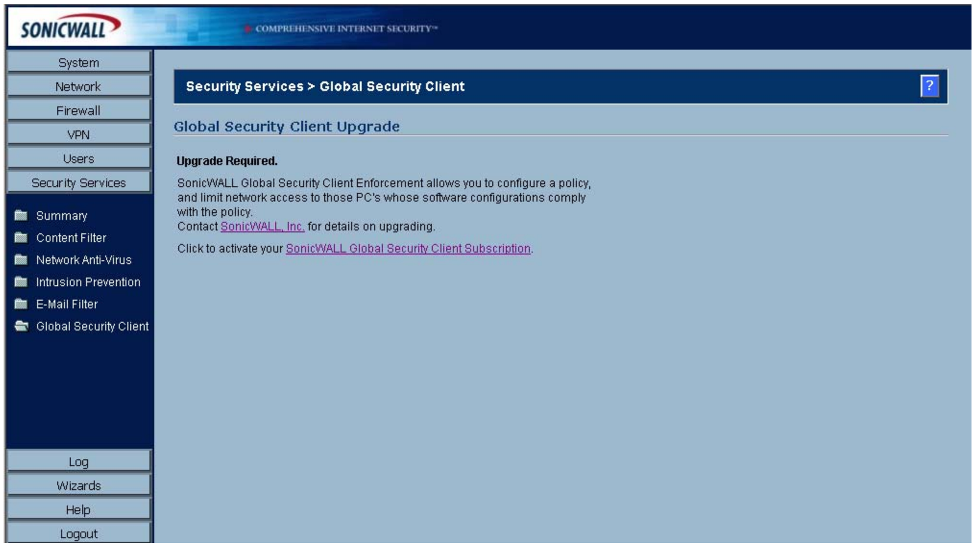
SonicWALL’s Distributed Enforcement Architecture (DEA) technology enables the policy enforcement capabilities that provide the framework for the Global Security Client’s complete security solution for all remote and network desktops. SonicWALL’s DEA technology enables the automatic installation of new software components, changes the configuration of different components, verifies version information, forces updates of components, informs the user which components do not meet the policy requirements, and provides user authentication for policy enforcement.

SonicWALL Global Security Client Activation

If you do not have SonicWALL Global Security Client activated on your SonicWALL security appliance, you must purchase SonicWALL Global Security Client from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you do not have SonicWALL Global Security Client installed on your SonicWALL security appliance, the **Security Services > Global Security Client** page indicates an upgrade is required and includes a link to activate your IPS subscription from the SonicWALL management interface.

Activating SonicWALL Global Security Client


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Security Services
Summary
Content Filter
Network Anti-Virus
Intrusion Prevention
E-Mail Filter
Global Security Client
Log
Wizards
Help
Logout
?

Security Services > Global Security Client

Global Security Client Upgrade

Upgrade Required.

SonicWALL Global Security Client Enforcement allows you to configure a policy, and limit network access to those PC's whose software configurations comply with the policy.
Contact SonicWALL, Inc. for details on upgrading.

Click to activate your SonicWALL Global Security Client Subscription.

If you have an Activation Key for your SonicWALL Global Security Client, follow these steps to activate the service:

1. Click the **SonicWALL Global Security Client Subscription** link on the **Security Services > Global Security Client** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Global Security Client Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL IPS subscription is activated on your SonicWALL security appliance.

If you activated the SonicWALL IPS subscription on mySonicWALL.com, the SonicWALL Global Security Client activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

PART 11

Log

CHAPTER 49

Viewing Log Events

SonicOS Log Event Messages Overview

During the operation of a SonicWALL security appliance, SonicOS software sends log event messages to the console. Event logging automatically begins when the SonicWALL security appliance is powered on and configured. SonicOS supports a traffic log containing entries with multiple fields.

Log event messages provide operational informational and debugging information to help you diagnose problems with communication lines, internal hardware, or your firmware configuration.

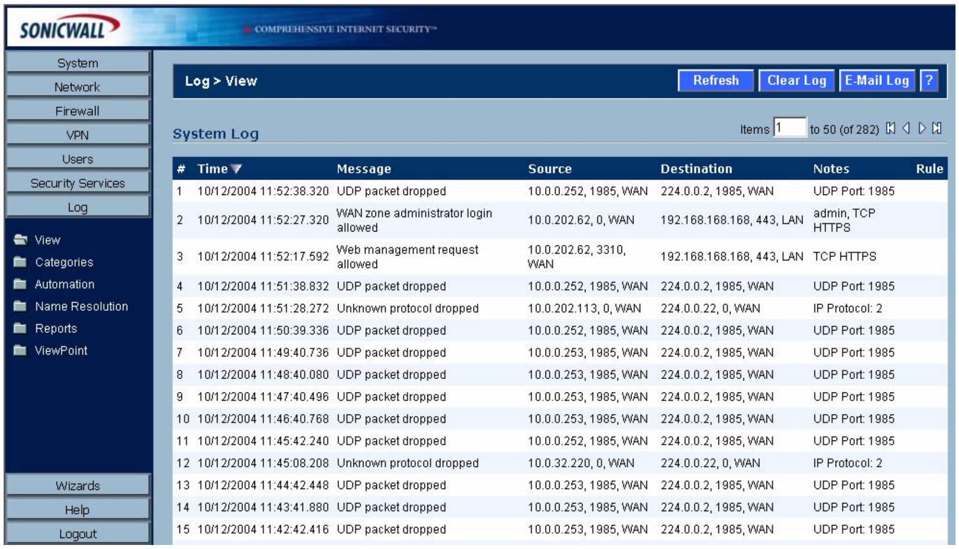
Note: *Not all log event messages indicate operational issues with your SonicWALL security appliance.*

The **Log > View** console display provides log event messages including the following fields for alert notification:

- **Time**—Displays the hour and minute the event occurred.
- **Priority**—Displays the level urgency for the event.
- **Category**—Displays the event type.
- **Message**—Displays a description of the event.
- **Source**—Displays the source IP address of incoming IP packet.
- **Destination**—Displays the destination IP address of incoming IP packet.
- **Note**—Displays displays additional information specific to a particular event occurrence.
- **Rule**—Displays the source and destination zones for the access rule. This field provides a link to the access rule defined in the ‘Firewall’ > ‘Access Rules’ page.

The display fields for a log event message provides you with data to verify your configurations, trouble-shoot your security appliance, and track IP traffic.

Log > View



#	Time	Message	Source	Destination	Notes	Rule
1	10/12/2004 11:52:38.320	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
2	10/12/2004 11:52:27.320	WAN zone administrator login allowed	10.0.202.62, 0, WAN	192.168.168.168, 443, LAN	admin, TCP HTTPS	
3	10/12/2004 11:52:17.592	Web management request allowed	10.0.202.62, 3310, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
4	10/12/2004 11:51:38.832	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
5	10/12/2004 11:51:28.272	Unknown protocol dropped	10.0.202.113, 0, WAN	224.0.0.22, 0, WAN	IP Protocol: 2	
6	10/12/2004 11:50:39.336	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
7	10/12/2004 11:49:40.736	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
8	10/12/2004 11:48:40.080	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
9	10/12/2004 11:47:40.496	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
10	10/12/2004 11:46:40.768	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
11	10/12/2004 11:45:42.240	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
12	10/12/2004 11:45:08.208	Unknown protocol dropped	10.0.32.220, 0, WAN	224.0.0.22, 0, WAN	IP Protocol: 2	
13	10/12/2004 11:44:42.448	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
14	10/12/2004 11:43:41.880	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
15	10/12/2004 11:42:42.416	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	

The SonicWALL security appliance maintains an **Event** log which displays potential security threats. This log can be viewed with a browser using the SonicWALL Web Management Interface, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

Click **Log** on the left side of the browser window. The default view is **Log > View**.

The SonicWALL security appliance provides logging, alerting, and reporting features, which can be viewed in the **Log** section of the SonicWALL Web Management Interface.

Note: *For a complete description of log messages, see the SonicWALL Log Event Reference Guide available at the SonicWALL documentation Web site <http://www.sonicwall.com/services/documentation.html>*

Navigating and Sorting Log View Table Entries

The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the navigation control bar located at the top right of the **Log View** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

SonicOS Log Entries

Each log entry contains the date and time of the event and a brief message describing the event. It is also possible to copy the log entries from the management interface and paste into a report. The SonicWALL security appliance manages log events in the following manner:

- **Dropped TCP, UDP, or ICMP packets**

  When IP packets are blocked by the SonicWALL security appliance, dropped TCP, UDP and ICMP messages are displayed. The messages include the source and destination IP addresses of the packet. The TCP or UDP port number or the ICMP code follows the IP address. Log messages usually include the name of the service in quotation marks.

- **Blocked Web Sites**

  When a computer attempts to connect to the blocked site or newsgroup, a log event is displayed. The computer's IP address, Ethernet address, the name of the blocked Web site, and the **Content Filter List Code** is displayed. Code definitions for the 12 Content Filter List categories are displayed in the table below:

1. Violence/Hate/Racism	5. Weapons	9. Illegal Skills/Questionable Skills
2. Intimate Apparel/ Swimsuit	6. Adult/Mature Content	10. Sex Education
3. Nudism	7. Cult/Occult	11. Gambling
4. Pornography	8. Drugs/Illegal Drugs	12. Alcohol/Tobacco

- **Blocked Java, etc**.

  When ActiveX, Java or Web cookies are blocked, messages with the source and destination IP addresses of the connection attempt is displayed.

- **Ping of Death, IP Spoof, and SYN Flood Attacks**

  The IP address of the machine under attack and the source of the attack is displayed. In most attacks, the source address shown is fake and does not reflect the real source of the attack.

✓ **Tip:** *Some network conditions can produce network traffic that appears to be an attack, even if no one is deliberately attacking the LAN. Verify the log messages with SonicWALL Tech Support before contacting your ISP to determine the source of the attack.*

Refresh

To update log messages, clicking the **Refresh** button.

Clear Log

Clicking **Clear Log** deletes the contents of the log.

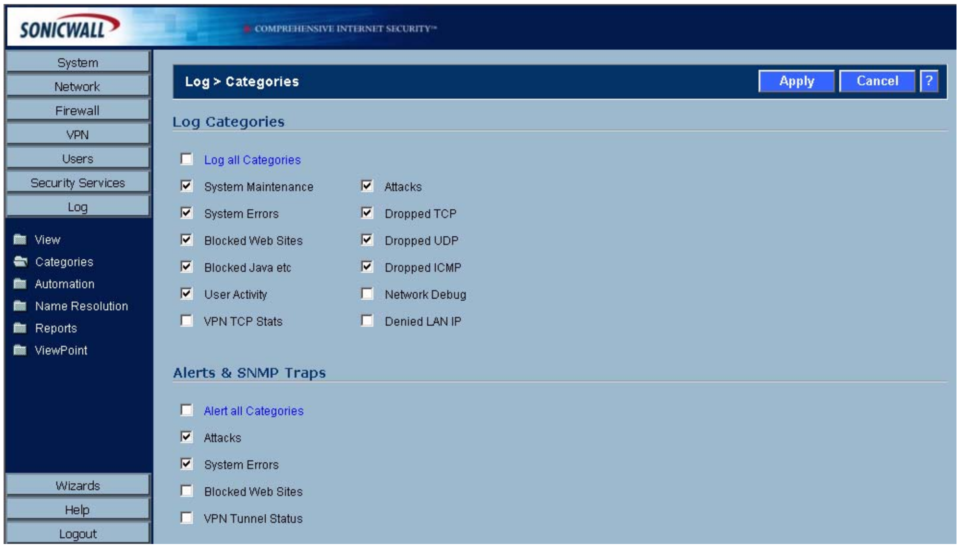
E-mail Log

If you have configured the SonicWALL security appliance to e-mail log files, clicking **E-mail Log** sends the current log files to the e-mail address specified in the **Log > Automation > E-mail** section.

CHAPTER 50

Specifying Log Categories

Log > Categories


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Users
Security Services
Log
View
Categories
Automation
Name Resolution
Reports
ViewPoint
Wizards
Help
Logout
Log > Categories
Apply
Cancel
?

Log Categories

☐ Log all Categories
☑ System Maintenance
☑ System Errors
☑ Blocked Web Sites
☑ Blocked Java etc
☑ User Activity
☐ VPN TCP Stats
☑ Attacks
☑ Dropped TCP
☑ Dropped UDP
☑ Dropped ICMP
☐ Network Debug
☐ Denied LAN IP

Alerts & SNMP Traps

☐ Alert all Categories
☑ Attacks
☑ System Errors
☐ Blocked Web Sites
☐ VPN Tunnel Status

You can define which log messages appear in the SonicWALL security appliance **Event Log**.

Log Categories

All **Log Categories** are enabled by default except **Network Debug**.

- **Log all Categories**
  Select **Log all Categories** to begin logging all event categories.
- **System Maintenance**
  Logs general system activity, such as system activations.
- **System Errors**
  Logs problems with DNS, or e-mail.
- **Blocked Web Sites**
  Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
- **Blocked Java, etc.**

Logs Java, ActiveX, and Cookies blocked by the SonicWALL security appliance.

- **User Activity**
  Logs successful and unsuccessful log in attempts.
- **VPN TCP Stats**
  Logs TCP connections over VPN tunnels.
- **System Environment (PRO 3060)**
  Logs events about fan failure, overheating, and any hardware issues.
- **Attacks**
  Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing.
- **Dropped TCP**
  Logs blocked incoming TCP connections.
- **Dropped UDP**
  Logs blocked incoming UDP packets.
- **Dropped ICMP**
  Logs blocked incoming ICMP packets.
- **Network Debug**
  Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. **Network Debug** information is intended for experienced network administrators.
- **Denied LAN IP**
  Logs all LAN IP addresses denied by the SonicWALL security appliance.

Alerts & SNMP Traps

Alerts are events, such as attacks, which warrant immediate attention. When events generate alerts, messages are immediately sent to the e-mail address defined in the **Send alerts to** field. **Attacks** and **System Errors** are enabled by default, **Blocked Web Sites** and **VPN Tunnel Status** are disabled.

- **Alert all Categories**
  Select **Alert all Categories** to begin logging of all alert categories.
- **Attacks**
  Log entries categorized as **Attacks** generate alert messages.
- **System Errors**
  Log entries categorized as **System Errors** generate alert messages.
- **Blocked Web Sites**
  Log entries categorized as **Blocked Web Sites** generate alert messages.
- **VPN Tunnel Status**
  Log entries categorized as **VPN Tunnel Status** generate alert messages.
- **System Environment (PRO 3060)**
  Logs events about fan failure, overheating, and any hardware issues.

Once you have configured the **Log Categories** window, click **Apply**. Once the SonicWALL security appliance is updated, a message confirming the update is displayed at the bottom of the browser window.

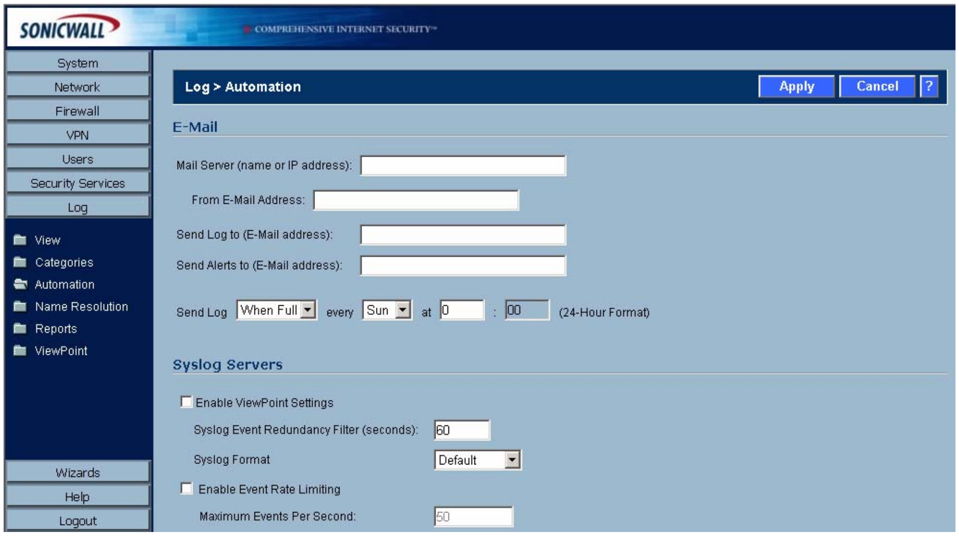
CHAPTER

51

Configuring Log Automation

Log > Automation

Click **Log**, and then **Automation** to begin configuring the SonicWALL security appliance to send log files using e-mail and configuring syslog servers on your network.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Users
Security Services
Log
View
Categories
Automation
Name Resolution
Reports
ViewPoint
Wizards
Help
Logout
Log > Automation
Apply
Cancel
?

E-Mail

Mail Server (name or IP address):

From E-Mail Address:

Send Log to (E-Mail address):

Send Alerts to (E-Mail address):

Send Log When Full every Sun at 0 : 00 (24-Hour Format)

Syslog Servers

☐ Enable ViewPoint Settings

Syslog Event Redundancy Filter (seconds): 60

Syslog Format: Default

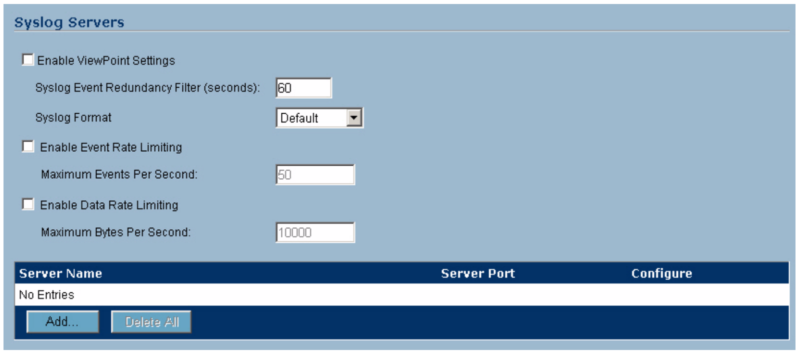
☐ Enable Event Rate Limiting

Maximum Events Per Second: 50

E-mail

- **Mail Server** - to e-mail log or alert messages, enter the name or IP address of your mail server in the **Mail Server** field. If this field is left blank, log and alert messages are not e-mailed.
- **Send Log To** - enter your full e-mail address in the **Send log to** field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL security appliance memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts To** - enter your full e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Enter a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.
- **Send Log** / **Every** / **At** - The **Send Log** menu determines the frequency of log e-mail messages: **Daily**, **Weekly**, or **When Full**. If the **Weekly** or **Daily** option is selected, then select the day of the week the e-mail is sent in the **Every** menu. If the **Weekly** or the **Daily** option is selected, enter the time of day when the e-mail is sent in the **At** field.

Syslog Servers



Syslog Servers

☐ Enable ViewPoint Settings

Syslog Event Redundancy Filter (seconds): 60

Syslog Format: Default

☐ Enable Event Rate Limiting

Maximum Events Per Second: 50

☐ Enable Data Rate Limiting

Maximum Bytes Per Second: 10000

Server Name	Server Port	Configure
No Entries		

In addition to the standard event log, the SonicWALL security appliance can send a detailed log to an external Syslog server. The SonicWALL security appliance Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL security appliance **Syslog** support requires an external server running a Syslog daemon on UDP Port 514.

Syslog Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the **Syslog** data.

To add syslog servers to the SonicWALL security appliance, click **Add**. The **Add Syslog Server** window is displayed.

1. Enter the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL security appliance are then sent to the servers. Up to three Syslog Server IP addresses can be added.
2. If your syslog is not using the default port of 514, enter the port number in the **Port Number** field.
3. Click **OK**.

If the SonicWALL security appliance is managed by SGMS, however, the **Syslog Server** fields cannot be configured by the administrator of the SonicWALL security appliance.

Syslog Event Redundancy Filter (seconds) - The **Syslog Event Redundancy Filter** setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred.

The **Syslog Event Redundancy Rate** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.

Syslog Format - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.

Enable ViewPoint Settings - Check this box to override Syslog settings, if you're using SonicWALL ViewPoint for your reporting solution.

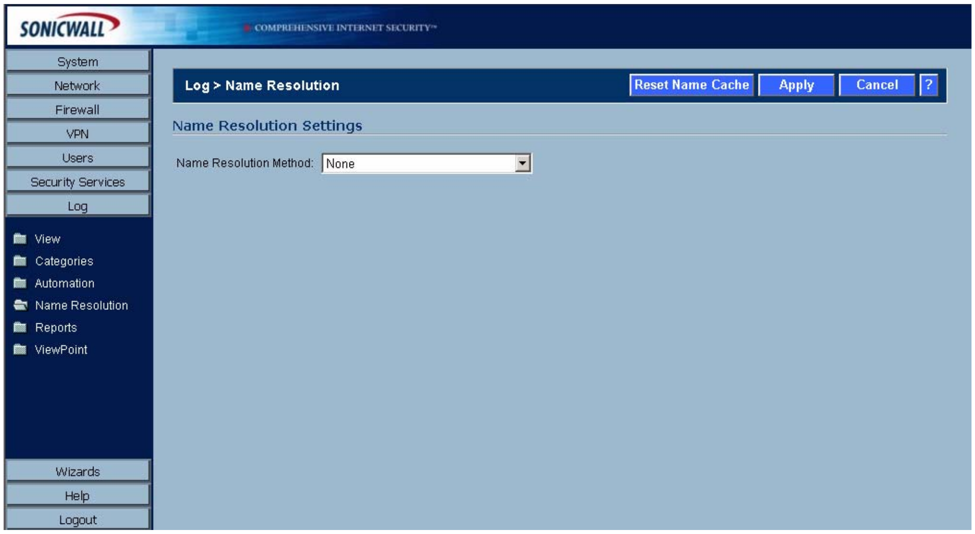
CHAPTER

52

Configuring Name Resolution

Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Security Services
Log
View
Categories
Automation
Name Resolution
Reports
ViewPoint
Wizards
Help
Logout
Log > Name Resolution
Reset Name Cache
Apply
Cancel
?

Name Resolution Settings

Name Resolution Method: None

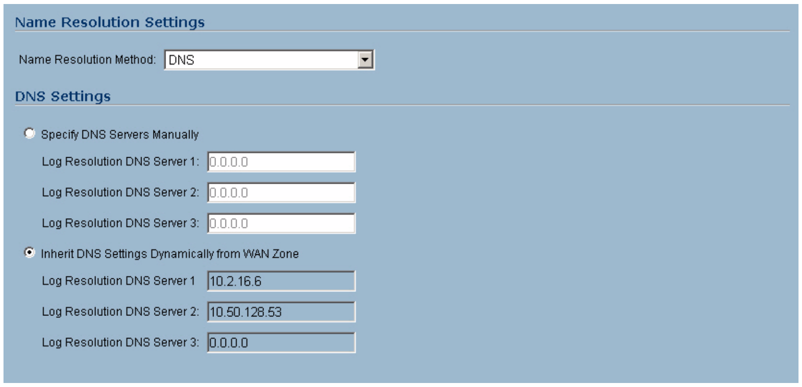
The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

Selecting Name Resolution Settings

The security appliance can use DNS, NetBios, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None**: The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS**: The security appliance will use the DNS server you specify to resolve addresses and names.



Name Resolution Settings

Name Resolution Method: DNS

DNS Settings

○ Specify DNS Servers Manually

Log Resolution DNS Server 1: 0.0.0.0

Log Resolution DNS Server 2: 0.0.0.0

Log Resolution DNS Server 3: 0.0.0.0

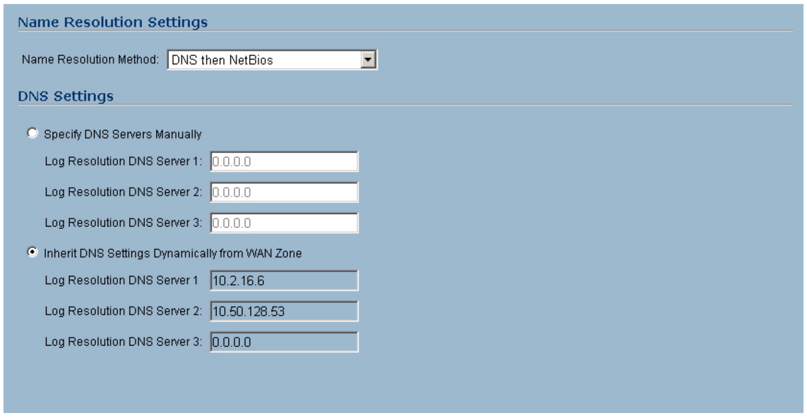
● Inherit DNS Settings Dynamically from WAN Zone

Log Resolution DNS Server 1 10.2.16.6

Log Resolution DNS Server 2: 10.50.128.53

Log Resolution DNS Server 3: 0.0.0.0

- **NetBios**: The security appliance will use NetBios to resolve addresses and names. If you select NetBios, no further configuration is necessary.
- **DNS then NetBios**: The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBios.



Name Resolution Settings

Name Resolution Method: DNS then NetBios

DNS Settings

○ Specify DNS Servers Manually

Log Resolution DNS Server 1: 0.0.0.0

Log Resolution DNS Server 2: 0.0.0.0

Log Resolution DNS Server 3: 0.0.0.0

● Inherit DNS Settings Dynamically from WAN Zone

Log Resolution DNS Server 1 10.2.16.6

Log Resolution DNS Server 2: 10.50.128.53

Log Resolution DNS Server 3: 0.0.0.0

Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

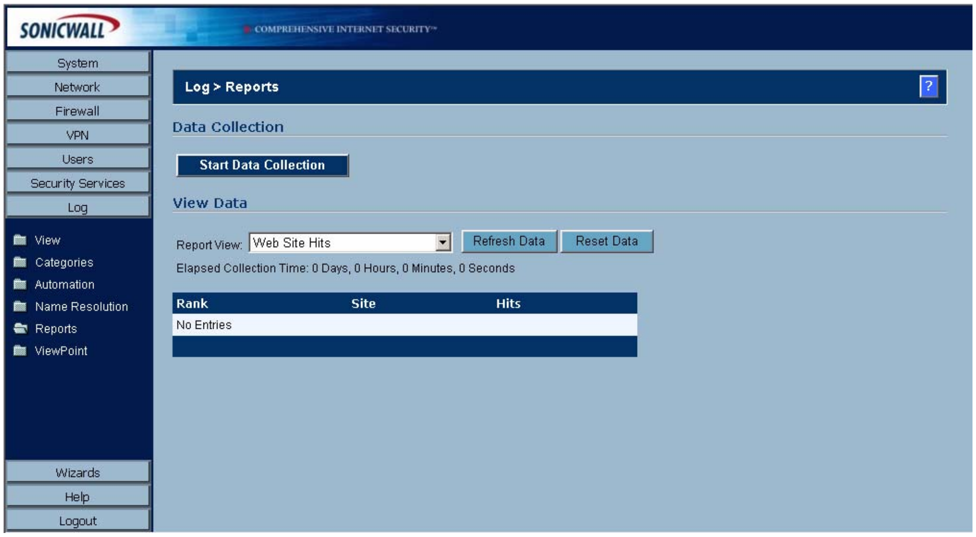
1. Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
2. If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
3. Click **Apply** in the top right corner of the **Log > Name Resolution** page to make your changes take effect.

CHAPTER

53

Generating and Viewing Log Reports

Log > Reports


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Firewall
VPN
Users
Security Services
Log
View
Categories
Automation
Name Resolution
Reports
ViewPoint
Wizards
Help
Logout
?
Start Data Collection
Refresh Data
Reset Data

Log > Reports

Data Collection

View Data

Report View: Web Site Hits

Elapsed Collection Time: 0 Days, 0 Hours, 0 Minutes, 0 Seconds

Rank	Site	Hits
No Entries		

The SonicWALL security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. Click **Log** on the left side of the browser window, and then click the **Reports**.

Data Collection

The **Reports** page includes the following functions and commands:

- **Start Data Collection**

  Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.
- **Reset Data**

Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the SonicWALL security appliance is restarted.

View Data

Select the desired report from the **Report to view** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

Web Site Hits

Selecting **Web Site Hits** from the **Report to view** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites.

Bandwidth Usage by IP Address

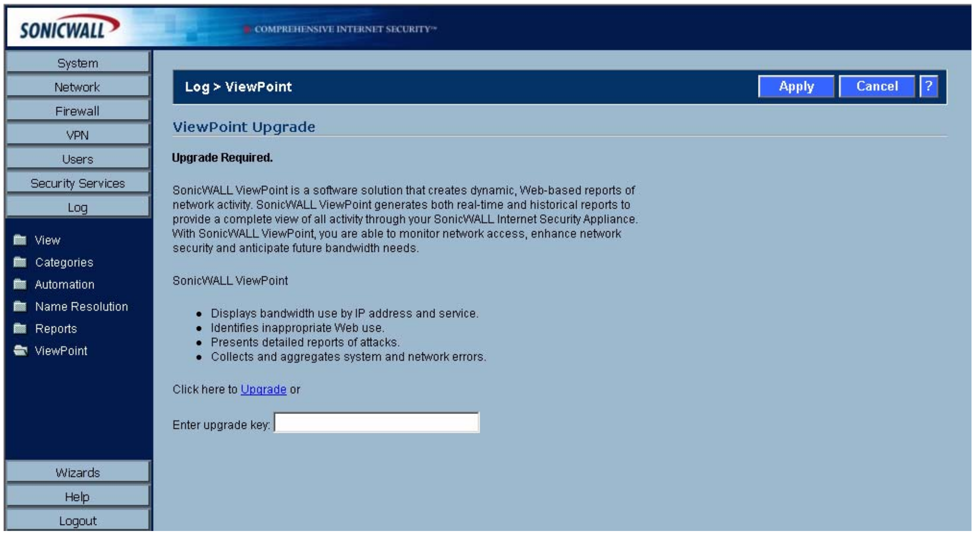
Selecting **Bandwidth Usage by IP Address** from the **Report to view** menu displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report to view** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

Log > ViewPoint


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Firewall
VPN
Users
Security Services
Log
View
Categories
Automation
Name Resolution
Reports
ViewPoint
Wizards
Help
Logout
Log > ViewPoint
Apply
Cancel
?

ViewPoint Upgrade

Upgrade Required.

SonicWALL ViewPoint is a software solution that creates dynamic, Web-based reports of network activity. SonicWALL ViewPoint generates both real-time and historical reports to provide a complete view of all activity through your SonicWALL Internet Security Appliance. With SonicWALL ViewPoint, you are able to monitor network access, enhance network security and anticipate future bandwidth needs.

SonicWALL ViewPoint

- Displays bandwidth use by IP address and service.
- Identifies inappropriate Web use.
- Presents detailed reports of attacks.
- Collects and aggregates system and network errors.

Click here to Upgrade or

Enter upgrade key:

SonicWALL ViewPoint

SonicWALL ViewPoint is a software solution that creates dynamic, Web-based reports of network activity. ViewPoint generates both real-time and historical reports to provide a complete view of all activity through your SonicWALL security appliance. With SonicWALL ViewPoint, you are able to monitor network access, enhance network security and anticipate future bandwidth needs.

- Displays bandwidth use by IP address and service.
- Identifies inappropriate Web use.
- Presents detailed reports of attacks.
- Collects and aggregates system and network errors.

Note: *For complete instructions on configuring and managing SonicWALL ViewPoint, see the SonicWALL ViewPoint User's Guide, available on the SonicWALl security appliance Resource CD or at <http://www.sonicwall.com/services/ViewPoint_documentation.html>.*

APPENDIX

A

Using the SonicSetup Diagnostic and Recovery Tool

SonicSetup

SonicSetup provides improved diagnostic and initial setup capabilities for SonicWALL security appliances. It demonstrates that a SonicWALl security appliance is in a functional state at the hardware, ROM, firmware, and user-interface levels, and that the SonicWALL security appliance can be successfully reached, administered, and configured.

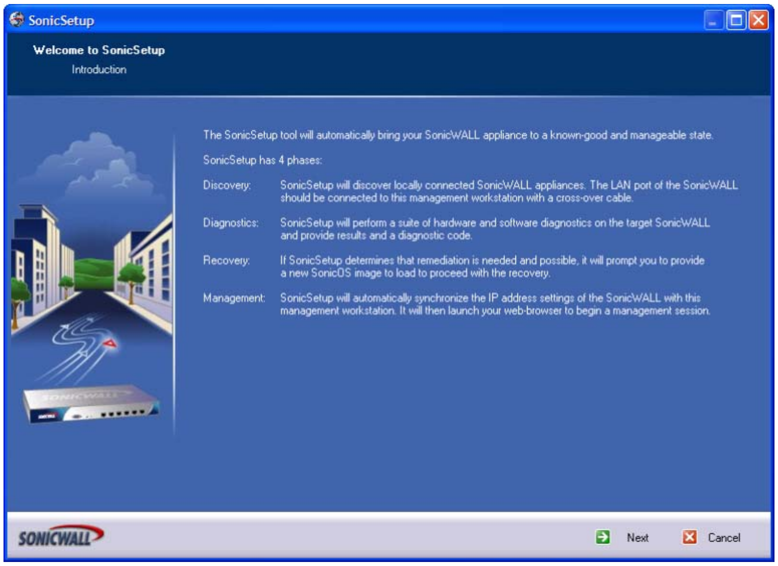
SonicSetup is a diagnostic and recovery tool, not a provisioning tool. It is intended to recover from unknown or corrupt states due to ROM, firmware, or preference file corruption, and to automate the synchronization of network addressing between the SonicWALL security appliance and the management workstation.

SonicSetup has two components: A SonicWALL ROM component, and a Win32 executable.

The recommended configuration for SonicSetup is direct connection between the SonicWALL appliance’s LAN port and the management workstation using a cross-over cable. SonicSetup uses layer 2 broadcasts to discover a SonicSetup-capable SonicWALL security appliance, but as a security measure, SonicSetup only makes changes to the configuration if the LAN port is the only active link on the SonicWALL security appliance; this is intended to prevent the use of SonicSetup on a production SonicWALL security appliance.

Introduction and Discovery

After establishing a connection between the SonicWALL and the management workstation (preferably with a direct cross-over cable connection), launch SonicSetup.exe. SonicSetup presents a brief introductory page explaining the recovery processes. Clicking the **Next** button begins the layer 2 discovery process, which should take less than 5 seconds.



Welcome to SonicSetup

Introduction

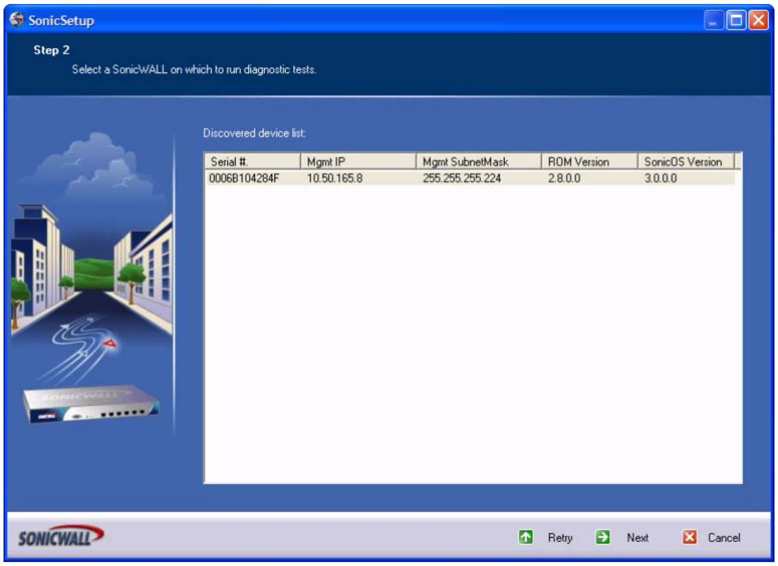
The SonicSetup tool will automatically bring your SonicWALL appliance to a known-good and manageable state.

SonicSetup has 4 phases:

Discovery:	SonicSetup will discover locally connected SonicWALL appliances. The LAN port of the SonicWALL should be connected to this management workstation with a cross-over cable.
Diagnostics:	SonicSetup will perform a suite of hardware and software diagnostics on the target SonicWALL and provide results and a diagnostic code.
Recovery:	If SonicSetup determines that remediation is needed and possible, it will prompt you to provide a new SonicOS image to load to proceed with the recovery.
Management:	SonicSetup will automatically synchronize the IP address settings of the SonicWALL with this management workstation. It will then launch your web-browser to begin a management session.

Device Selection

SonicSetup displays the discovered device(s), and then awaits the selection of a device on which to run system diagnostics.



Step 2

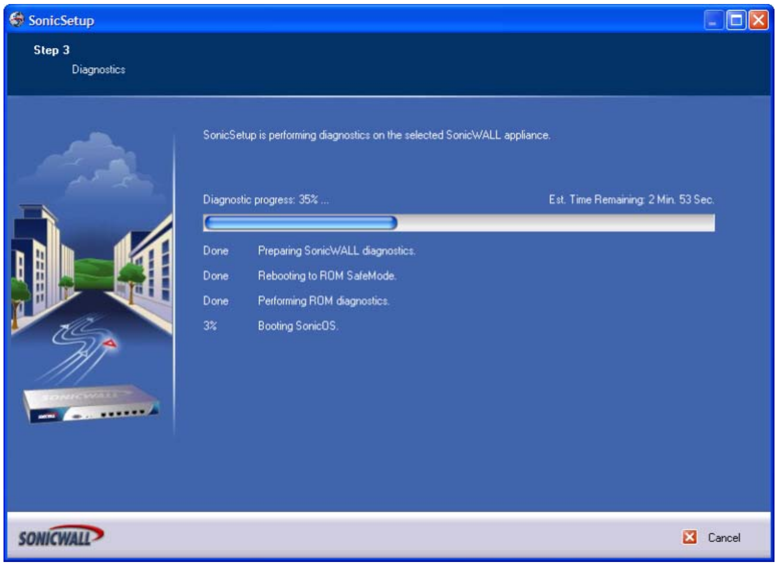
Select a SonicWALL on which to run diagnostic tests.

Discovered device list:

Serial #.	Mgmt IP	Mgmt SubnetMask	ROM Version	SonicOS Version
0006B104284F	10.50.165.8	255.255.255.224	2.8.0.0	3.0.0.0

Diagnostics

Diagnostics include hardware and software components, and it runs in two modes: ROM and Firmware. The transition between the two modes is automatically controlled by SonicSetup, and is transparent to the administrator.



SonicSetup is performing diagnostics on the selected SonicWALL appliance.

Diagnostic progress: 35% ... Est. Time Remaining: 2 Min. 53 Sec.

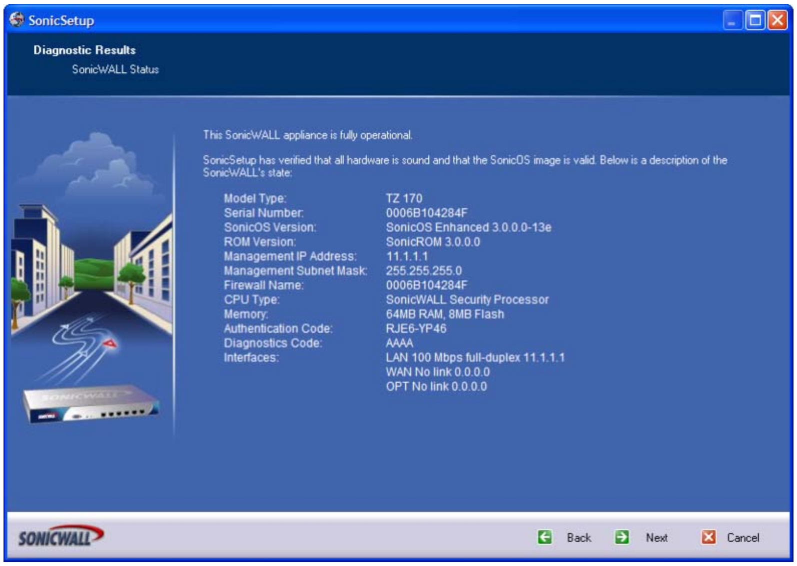
Done Preparing SonicWALL diagnostics.
Done Rebooting to ROM SafeMode.
Done Performing ROM diagnostics.
3% Booting SonicOS.

Diagnostics include (component and mode noted in parenthesis):

- **Interface Test** – Demonstrates operability of the LAN interface by means of discovery. (Hardware, Implicit)
- **Validate ROM** – Verifies that the ROM checksum stored in flash matches the calculated checksum. (Hardware, ROM)
- **Firmware Flash Region Test** – Performs sector verification on the area in flash memory in which the firmware is stored. Only run in the event of firmware corruption. (Hardware, ROM)
- **Wireless Radio Test** – Tests the wireless radio component of SonicWALL appliances with an integrated 802.11 radio. (Hardware, ROM)
- **Modem Test** – Tests the modem component of SonicWALL appliances with an integrated modem. (Hardware, ROM)
- **Firmware Validation** – Verifies the state of firmware by validating the header and performing a CRC check on the data. If the validation fails, the Firmware Flash Region test is flagged to run. (Software, ROM)
- **Bootlog Analysis** – While the firmware starts, the startup messages (typically displayed on the console) are written to a protected region of memory. The SonicWALL security appliance is allotted a certain time to complete the boot process which, if exceeded, triggers a reboot. If the boot process fails again, the device reboots into SafeMode. From SafeMode, SonicSetup retrieves the bootlog and will determine the point of failure. (Software, Firmware).

Diagnostic Results

After the diagnostics have run, the diagnostic results are displayed:



Diagnostic Results
SonicWALL Status

This SonicWALL appliance is fully operational.

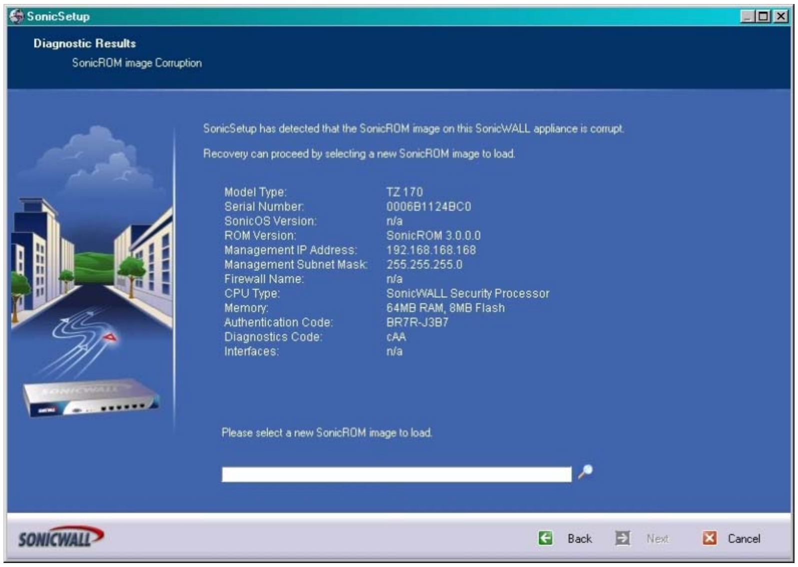
SonicSetup has verified that all hardware is sound and that the SonicOS image is valid. Below is a description of the SonicWALL's state:

Model Type:	TZ 170
Serial Number:	0006B104284F
SonicOS Version:	SonicOS Enhanced 3.0.0.0-13e
ROM Version:	SonicROM 3.0.0.0
Management IP Address:	11.1.1.1
Management Subnet Mask:	255.255.255.0
Firewall Name:	0006B104284F
CPU Type:	SonicWALL Security Processor
Memory:	64MB RAM, 8MB Flash
Authentication Code:	RJE6-YP46
Diagnostics Code:	AAAA
Interfaces:	LAN 100 Mbps full-duplex 11.1.1.1 WAN No link 0.0.0.0 OPT No link 0.0.0.0

Included in the results is the Diagnostic Code which, in the event of a failure, must be interpreted by SonicWALL Support. This code will contain specific information about the state of the SonicWALL security appliance's ROM and hardware. In the event of a non-recoverable ROM failure or a hardware failure, an RMA is the immediate course of action. Non-hardware failures (including some ROM failure states) are recoverable using SonicSetup.

SonicROM Recovery

If the SonicROM image is found to be corrupt, but is sufficiently functional to communicate with SonicSetup, the administrator is prompted to select a ROM image to load onto the unit. The ROM will be transferred to the SonicWALL security appliance by SonicSetup using a reliable layer 2 transport.



Diagnostic Results
SonicROM image Corruption

SonicSetup has detected that the SonicROM image on this SonicWALL appliance is corrupt.

Recovery can proceed by selecting a new SonicROM image to load.

Model Type:	TZ 170
Serial Number:	0006B1124BC0
SonicOS Version:	n/a
ROM Version:	SonicROM 3.0.0.0
Management IP Address:	192.168.168.168
Management Subnet Mask:	255.255.255.0
Firewall Name:	n/a
CPU Type:	SonicWALL Security Processor
Memory:	64MB RAM, 8MB Flash
Authentication Code:	BR7R-J3B7
Diagnostics Code:	cAA
Interfaces:	n/a

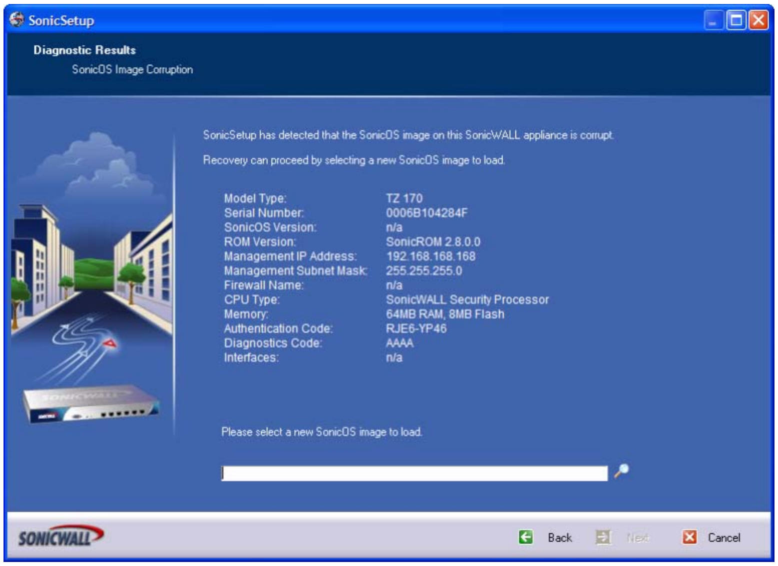
Please select a new SonicROM image to load.

If the SonicROM image fails to transfer, a failure notification page is displayed, and the administrator must have the opportunity to retry the process. Multiple failed attempts receive an appropriate response from SonicWALL Support.

After the new SonicROM image has been transferred to the SonicWALL security appliance, the image is written to flash, and the diagnostic process is run.

SonicOS Recovery

If the SonicOS image is found to be corrupt, the administrator is prompted to select a firmware image to load onto the SonicWALL security appliance. The firmware is then transferred to the SonicWALL by SonicSetup using a reliable layer 2 transport.



SonicSetup has detected that the SonicOS image on this SonicWALL appliance is corrupt.

Recovery can proceed by selecting a new SonicOS image to load.

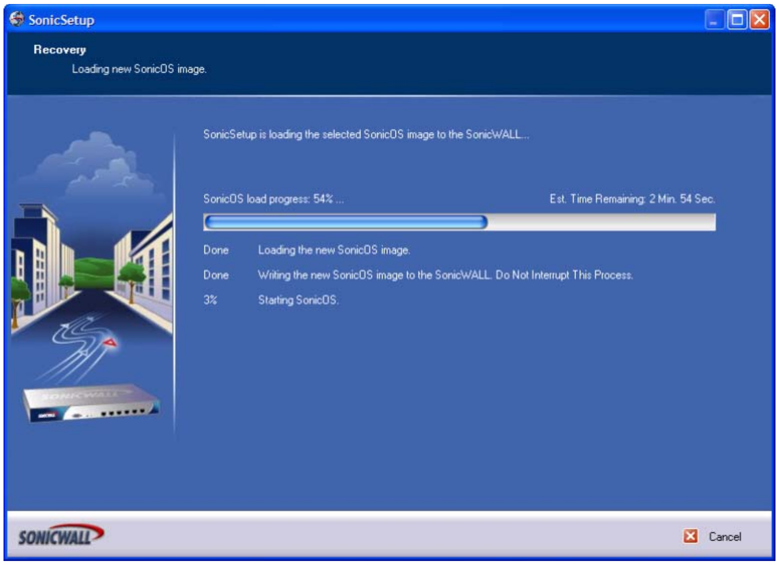
Model Type:	TZ 170
Serial Number:	0006B104284F
SonicOS Version:	n/a
ROM Version:	SonicROM 2.8.0.0
Management IP Address:	192.168.168.168
Management Subnet Mask:	255.255.255.0
Firewall Name:	n/a
CPU Type:	SonicWALL Security Processor
Memory:	64MB RAM, 8MB Flash
Authentication Code:	RJE6-YP46
Diagnostics Code:	AAAA
Interfaces:	n/a

Please select a new SonicOS image to load.

If the SonicOS image fails to transfer, a failure notification page is presented, and the administrator has the opportunity to retry the process. Multiple failed attempts receive an appropriate response from SonicWALL Support.

After the new SonicOS image is transferred to the SonicWALL security appliance, the image is written to flash, and then SonicOS is restarted.

Note: *It takes approximately 5 minutes to transfer either a ROM or firmware image, write the image to flash, and restart the SonicWALL security appliance. It is critical that during this phase there is no interruption of network connectivity between the SonicSetup workstation and the SonicWALL security appliance, the SonicSetup executable is not terminated, and the power to the SonicWALL security appliance is not interrupted.*



Recovery

Loading new SonicOS image.

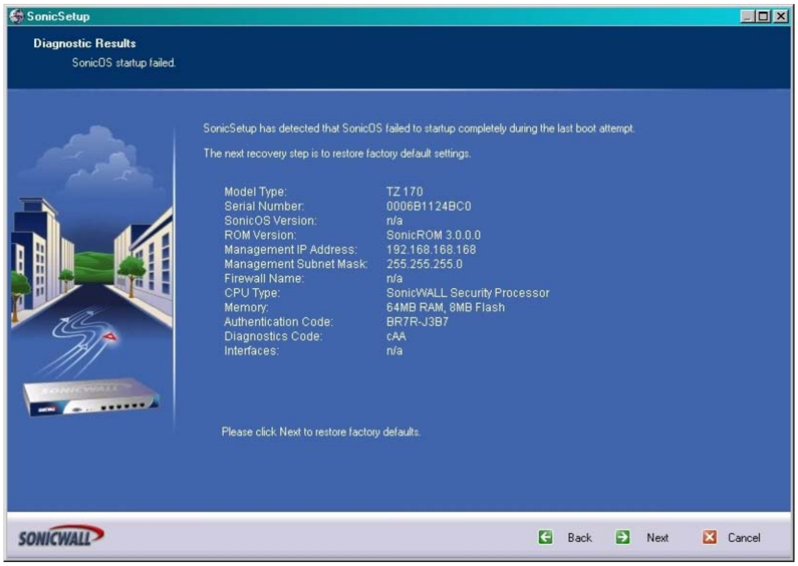
SonicSetup is loading the selected SonicOS image to the SonicWALL...

SonicOS load progress: 54% ... Est. Time Remaining: 2 Min. 54 Sec.

Done Loading the new SonicOS image.
Done Writing the new SonicOS image to the SonicWALL. Do Not Interrupt This Process.
3% Starting SonicOS.

Restoring Factory Defaults

If the SonicWALL fails to startup completely after loading the new SonicOS image (and attempting to start with the existing configuration/prefs settings), a startup-failure notification is displayed. The SonicSetup's next step is to restore factory defaults:



Diagnostic Results

SonicOS startup failed.

SonicSetup has detected that SonicOS failed to startup completely during the last boot attempt.

The next recovery step is to restore factory default settings.

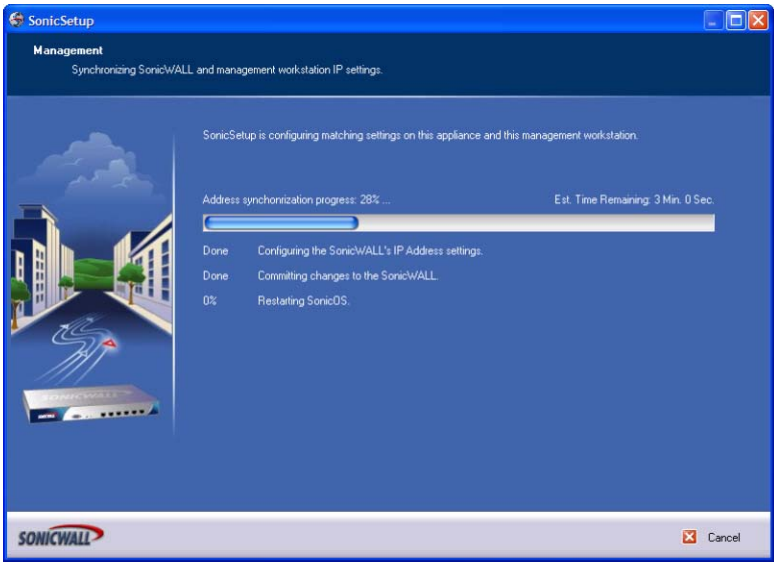
Model Type: TZ 170
Serial Number: 0006B1124BC0
SonicOS Version: n/a
ROM Version: SonicROM 3.0.0.0
Management IP Address: 192.168.168.168
Management Subnet Mask: 255.255.255.0
Firewall Name: n/a
CPU Type: SonicWALL Security Processor
Memory: 64MB RAM, 8MB Flash
Authentication Code: BR7R-J3B7
Diagnostics Code: cAA
Interfaces: n/a

Please click Next to restore factory defaults.

If SonicSetup fails to restore the SonicWALL to factory defaults, a failure notification page is displayed, and the administrator has the opportunity to retry the process. Multiple failed attempts receive an appropriate response from SonicWALL Support.

Address Synchronization

The SonicWALL should be fully operational at this time. The administrator is then prompted to provide an IP address for the SonicWALL:



SonicSetup

Management

Synchronizing SonicWALL and management workstation IP settings.

SonicSetup is configuring matching settings on this appliance and this management workstation.

Address synchonrization progress: 28% ...

Est. Time Remaining: 3 Min. 0 Sec.

Done Configuring the SonicWALL's IP Address settings.

Done Committing changes to the SonicWALL.

0% Restarting SonicOS.

- Any address may be set, regardless of the current IP address setting (i.e. the address may be set even if it is not currently at the default 192.168.168.168 setting, providing that only the LAN link on the SonicWALL security appliance is active).
- If the management workstation is statically or dynamically configured (with an existing lease) and the subnet is the same as that which was provided for the SonicWALL security appliance, no change will be made to the workstation's IP settings.
- If the management workstation is statically or dynamically configured (with an existing lease) and the subnet is different from the SonicWALL security appliance's subnet, an IP address matching the subnet just assigned to the SonicWALL is bound as a secondary address to the workstation. For example, if the management workstation has a dynamically assigned IP address of 10.50.165.13, and the SonicWALL security appliance was configured to 11.1.1.1, SonicSetup binds the additional address of 11.1.1.254 to the management workstation. Management workstation IP address synchronization is performed by SonicSetup decrements (or increments, as needed) of the last octet assigned to the SonicWALL security appliance, and assigns the first available address to the management workstation; upon reboot or network card re-initialization, this additional binding is cleared:

```
Ethernet adapter intel:

        Physical Address. . . . . . . . . : 08-00-46-A2-EB-4D
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 11.1.1.254
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 10.50.165.13
        Subnet Mask . . . . . . . . . . . : 255.255.255.224
        Default Gateway . . . . . . . . . : 10.50.165.1
        DHCP Server . . . . . . . . . . . : 10.50.165.2
        DNS Servers . . . . . . . . . . . : 10.50.165.2
                                            10.50.128.52
      Lease Obtained. . . . . . . . . . : Wednesday, November 03, 1402 9:59:42 PM
      Lease Expires . . . . . . . . . . : Thursday, November 04, 1402 5:59:42 AM
```

- A web-browser will be launched on the management workstation, and targets the management IP of the SonicWALL security appliance.
- The administrator can then log into, and configure the operational SonicWALL security appliance.

APPENDIX B

Resetting the SonicWALL Security Appliance Using SafeMode

SonicWALL SafeMode

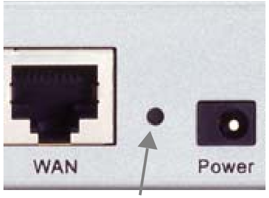
If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SonicWALL security appliance security appliance's SafeMode is a simplified management interface that enables you to:

- Make a backup copy of your current settings
- Reboot the security appliance with your current settings
- Reboot the security appliance with factory default settings
- Reboot the security appliance with settings from your backup
- Upgrade SonicOS Firmware

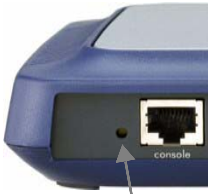
To reset the SonicWALL security appliance, perform the following steps:

1 Connect your management station to a LAN port on the SonicWALL security appliance and configure you management station IP address to **192.168.168.20**.

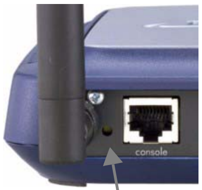
2 Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the back of the security appliance for five to ten seconds. The reset button is in a small hole next to the console port.or next to the power supply:



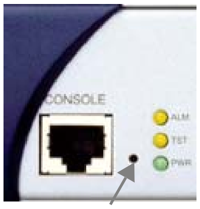
Reset button
TZ 50, TZ 150



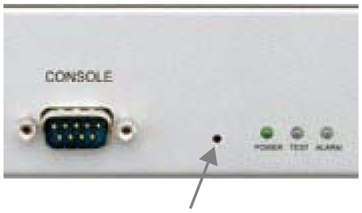
Reset button
TZ 170, TZ 170 SP



Reset button
TZ 170 Wireless

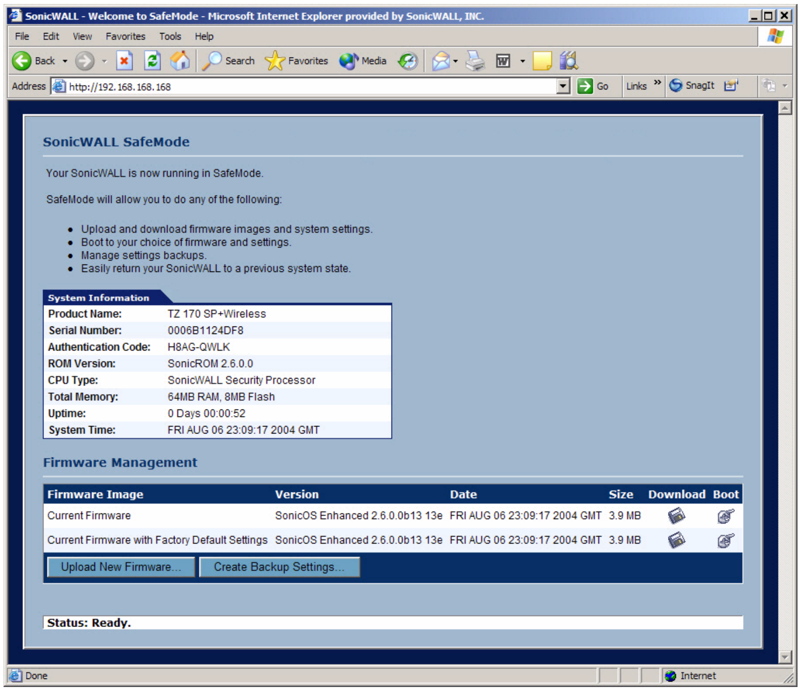


Reset button
PRO 1260



Reset button
PRO 2040, PRO 3060

3. The **Test** light starts blinking when the security appliance has rebooted into SafeMode.
4. Connect to the management interface: Point the Web browser on your Management Station to **192.168.168.168**. The SafeMode management interface displays:


SonicWALL - Welcome to SafeMode - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.168
Go Links SnagIt
Upload New Firmware...
Create Backup Settings...
Done
Internet

SonicWALL SafeMode

Your SonicWALL is now running in SafeMode.

SafeMode will allow you to do any of the following:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and settings.
- Manage settings backups.
- Easily return your SonicWALL to a previous system state.

System Information	
Product Name:	TZ 170 SP+Wireless
Serial Number:	0006B1124DF8
Authentication Code:	H8AG-QWLK
ROM Version:	SonicROM 2.6.0.0
CPU Type:	SonicWALL Security Processor
Total Memory:	64MB RAM, 8MB Flash
Uptime:	0 Days 00:00:52
System Time:	FRI AUG 06 23:09:17 2004 GMT

Firmware Management

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 2.6.0.0b13 13e	FRI AUG 06 23:09:17 2004 GMT	3.9 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 2.6.0.0b13 13e	FRI AUG 06 23:09:17 2004 GMT	3.9 MB		

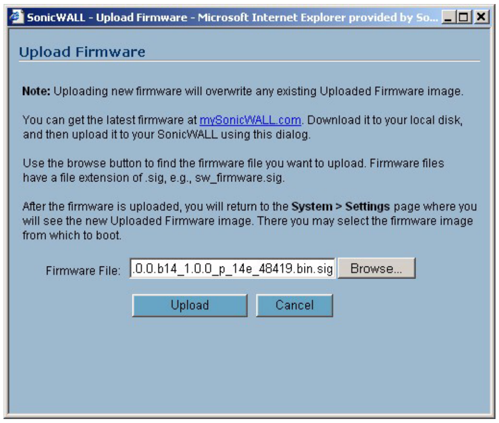
Status: Ready.

5. If you have made any configuration changes to the security appliance, make a backup copy of your current settings. Click **Create Backup Settings**.
6. First try rebooting the security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.
7. After the SonicWALL security appliance has rebooted, try to open the management interface again.
8. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again.
9. In SafeMode, restart the firmware with the factory default settings. Click the boot icon in the same line with **Current Firmware with Factory Default Settings**.
10. After the SonicWALL security appliance has rebooted, try to open the management interface again.
11. If you are able to connect, you can recreate your configuration or try to reboot with the backup settings: Restart the security appliance in SafeMode again, and click the boot icon in the same line with **Current Firmware with Backup Settings**.

Upgrading SonicOS Firmware

In SafeMode, you can upload newer versions of the SonicOS firmware to your SonicWALL security appliance.

1. Connect to <http://www.mysonicwall.com>. If you have already registered your security appliance, you should be automatically notified of any upgrades available for your model.
2. Copy the new firmware to a directory on your management station.
3. If the SonicWALL security appliance is not already in safe mode, press and hold the reset button to restart the security appliance in SafeMode.
4. At the bottom of the page, click **Upload New Firmware**.



SonicWALL - Upload Firmware - Microsoft Internet Explorer provided by So...

Upload Firmware

Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

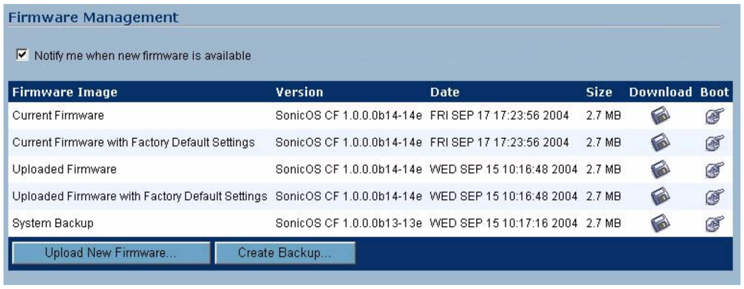
You can get the latest firmware at mySonicWALL.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

After the firmware is uploaded, you will return to the **System > Settings** page where you will see the new Uploaded Firmware image. There you may select the firmware image from which to boot.

Firmware File: .0.0.b14_1.0.0_p_14e_48419.bin.sig

5. In the **Upload Firmware** page, click **Browse** to locate and select the new firmware file.
6. Click **Upload**.
7. The list under Firmware Management now shows the current firmware and the newly uploaded firmware with your current settings, factory default settings, and backup settings.



Firmware Management

☑ Notify me when new firmware is available

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS CF 1.0.0.0b14-14e	FRI SEP 17 17:23:56 2004	2.7 MB		
Current Firmware with Factory Default Settings	SonicOS CF 1.0.0.0b14-14e	FRI SEP 17 17:23:56 2004	2.7 MB		
Uploaded Firmware	SonicOS CF 1.0.0.0b14-14e	WED SEP 15 10:16:48 2004	2.7 MB		
Uploaded Firmware with Factory Default Settings	SonicOS CF 1.0.0.0b14-14e	WED SEP 15 10:16:48 2004	2.7 MB		
System Backup	SonicOS CF 1.0.0.0b13-13e	WED SEP 15 10:17:16 2004	2.7 MB		

You can boot the security appliance from whichever one you want. Click the boot icon ☞ in the same line with the firmware and settings you want to apply to the security appliance.

Index

Numerics
802.11g 127
A
access point status 136
access rules
    bandwidth management 180
    configuration examples 187
    general rule wizard 182
    overview 179
    public server rule wizard 181
    restoring defaults 181
    rule wizard 181
account lifetime 133
accounts
    wireless guest services 171
activating Gateway Anti-Virus 281
activating Gateway Anti-Virus free trial version 282
administration 39
    changing the default size of tables 41
    firewall name 40
    login security 40
    name and password 40
    SNMP 42
    SonicWALL Global Management System 43
    web management settings 41
ARP 93
    ARP cache table 97
    flushing ARP cache 97
associated stations 136
authentication type 148
B
beaconing 151
bypass guest authentication 166
C
channel 136, 141
comment 133
configuration wizard 30
custom login page 168
D
DAT, see dynamic address translation
deployment scenarios
    guest internet gateway 18
    office gateway 18
    secure access point 18
    secure wireless bridge 18
DHCP server 99
    configuring dynamic ranges 100
    current DHCP leases 102
    lease scopes 100
    settings 99
    static entries 101
diagnostics 51
    active connections monitor 53
    CPU monitor 54
    DNS name lookup 54
    find network path 55
    packet trace 55
    ping 57
    process monitor 57
    reverse name resolution 57
    tech support report 52
discards 137
    bad WEP key 137
DTIM interval 153
dynamic address translation 166
dynamic DNS 103
    configuring 105
    providers 103
E
EAP, see extensible authentication protocol
easy ACL 130
extensible authentication protocol 148, 149
F
FCS errors 137
firewall
    advanced settings 189
    dynamic ports 190
    force FTP data connections port 20 190
    H.323 protocol 193
    NetBIOS pass through 189
    non-SIP packets on signaling port 195
    randomize IP ID 190
    services 191
    SIP 193
    SIP media 195
    SIP signaling 195
    source routed packets 190
    stealth mode 190
    TCP checksum 190
    TCP inactivity timeout 190
    transforming SIP messages 195
    user defined services 191
    VoIP 193
firmware management 48
    booting firmware 50
    notification 48
    SafeMode 49

- updating firmware 48
flexible default route 174
fragmentation threshold 153
fragments 137

G

Gateway Anti-Virus 279
- application control 280
- deep packet inspection 280
- features 280
- inter-zone scanning 280
- intrusion prevention 280
- signatures 280

guest account profiles 169
guest accounts 171
guest internet gateway 18, 21
guest profiles 169
guest services 163, 165, 171
- guest profile 169

H

H.323
- transforming H.323 messages 195

I

IEEE 802.11b 127
IEEE 802.11g 127
interclient communications 152
IP address deny list 167
ISP information for setup 9

L

LAN interface
- configuring 70
- Ethernet settings 71
- multiple subnets 70

log
- alerts 302
- categories 301
- configuring e-mail alerts 304
- e-mail log files 299
- messages 299
- name resolution 307
- reports 309
- SNMP traps 302
- SonicWALL ViewPoint 311
- syslog servers 304
- viewing log events 298

M

MAC address 136
MAC address list 156
MAC filter list 130, 155
MAC filtering 135
management interface 4
- accessing 11
- applying changes 6
- common icons 7
- getting help 7
- logging out 7
- navigating 5
- navigating tables 6
- status bar 5
- submenus 5

maximum concurrent guests 169
multicast frames 137
multiple retry frames 137

N

network
- DHCP server 99
- intranet 87
- routing 89
- static routes 90

network settings
- DNS 63
- interfaces 61
- interfaces table 62
- LAN properties 70
- NAT with DHCP client 66
- NAT with L2TP client 67
- NAT with PPPoE client 67
- NAT with PPTP client 68
- transparent mode 64, 72, 74
- wlan properties 79

node licensing
- currently licensed 34
- exclusion list 34
- status 34

O

office gateway 18
one-to-one NAT 81
- example 82

open system 148

P

post authentication redirect 169
preamble length 153
pre-shared key 148
PSK, see pre-shared key

R

resetting the CSM 2100 CF 321
restart SonicWALL security appliance 58
restore default settings 153
retry limit exceeded 137
routing
- configuring static routes 90
- route advertisement 91
- route advertisement configuration 91
- static route example 90
- table 92
- wireless guest services 175

RTS threshold 153

S

safemode 321

secure access point 18, 20
secure wireless bridge 18
security services
    activating a free trial of Intrusion Prevention Service 289
    activating Content Filtering Service 266
    activating Global Security Client 292
    activating Intrusion Prevention Service 288
    activating Network Anti-Virus 276
    blocked message 269
    free trials 36
    manage services online 36
    mandatory filtered IP addresses 273
    manual upgrade 36
    manual upgrade for closed environments 36
    mySonicWALL.com 262
    restrict web features 268
    SonicWALL Content Filtering Service 265
    SonicWALL E-Mail Filter 278
    SonicWALL Global Security Client 292
    SonicWALL Intrusion Prevention Service 285
    SonicWALL Network Anti-Virus 275
    summary table 35
    trusted domains 269
session timeout 133
setup wizard 11
    DHCP configuration 14
    PPPoE configuration 14
    PPTP configuration 15
    static IP configuration 12
shared key 148
signal retry frames 137
SMTP redirect 167
SonicWALL Gateway Anti-Virus/Intrusion Prevention Service 279
SSID 136
SSID controls 151
status 29
    latest alerts 31
    security services 31
    system information 30
    system messages 30
    wireless 135
system licenses 33

T

technical support xvii
time and date settings 45
transmit power 153

U

unicast frame 137
upgrading firmware 323
URL allow list 167
users
    acceptable use policy 252
    active user sessions 250
    adding users to SonicWALL database 257
    authentication 249
    authentication exclusions 251
    authentication methods 250
    global user settings 251
    guest profile 169
    RADIUS authentication 253

V

VPN
    3rd party certificates 241
    active VPN tunnels 203
    advanced settings 229
        fragmented packet handling 229
        IKE dead peer detection 230
        keep alive 230
        NAT traversal 229
        NetBIOS broadcasts 229
    certificate authority certificates 244
    configuring bandwidth management 231
    configuring site-to-site VPN connections 213
    configuring SonicWALL GroupVPN 203
    creating a IKE with 3rd party certificates site-to-site policy 219
    creating a manual key site-to-site policy 218
    creating an IKE using preshared secret site-to-site policy 216
    creating site-to-site policies using the VPN Policy window 220
    DHCP over VPN 233
        central gateway 234
        remote gateway 235
    exporting a GroupVPN policy 213
    L2TP server 237
    local certificates 242
    site-to-site VPN planning sheet 214
    SonicWALL Global Security Client 201
    SonicWALL Global VPN Client 201
    user authentication settings 230
    VPN policy wizard 215
    X.509 v3 certificate support 241

W

WAN interface 64
    Ethernet settings 68
    NAT enabled 64, 71, 73
    NAT with DHCP client 64
    NAT with L2TP client 64
    NAT with PPPoE 64
    NAT with PPTP client 64
    transparent mode 64, 71, 73
web proxy 85
    bypass on server failure 86
    configuring 86
WEP encryption 135
WEP key
    alphanumeric 148

    - hexadecimal. 148
- WEP key mode 148
- WGS, see wireless guest services
- WiFiSec 127, 136
- WiFiSec enforcement 130, 140
- WiFiSec Protected Access 148
    - EAP 149
    - PSK 149
- wireless
    - guest internet gateway 18
    - office gateway 18
    - secure access point 18
    - secure wireless bridge 18
    - WPA 148
- wireless access point 174
- wireless client communications 135
- wireless firmware 136
- wireless guest services 136, 163, 171
    - access point 174
    - account lifetime 133
    - account profiles 169
    - accounts 171
    - custom login page 168
    - dynamic address translation 166
    - flexible default route 174
    - in wireless chapter 129
    - IP address deny list 167
    - maximum concurrent guests 169
    - post authentication redirect 169
    - settings 165
    - SMTP redirect 167
    - url allow list 167
    - virtual adapter 174
    - wizard 133
- wireless node count 130
- wireless status 135
- wireless wizard 131
- wizards
    - wireless wizard 131
- WLAN 136
    - IP address 136
    - settings 136
    - statistics 137
    - subnet mask 136
- WPA encryption 148
- WPA, see WiFiSec Protected Access

SonicWALL,Inc.
1143 Borregas Avenue
Sunnyvale,CA 94089-1306

T: 408.745.9600
F: 408.745.9300

www.sonicwall.com

© 2004 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/ or registered trademarks of their respective companies. Specifications and descriptions subject to change with out notice.

P/ N 232- 000609- 00
Rev E 02/05